NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

JOINT APPLIED PROJECT

The Program Management Challenges of Web 2.0

By: **Yonghee K. Woodall**

June 2010

Advisors: **Brad R. Naegle**
Michael Boudreau

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** June 2010	**3. REPORT TYPE AND DATES COVERED** Joint Applied Project	
4. TITLE AND SUBTITLE The Program Management Challenges of Web 2.0			**5. FUNDING NUMBERS**
6. AUTHOR(S) Yonghee K. Woodall			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number: _____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

In this Joint Applied Project, the author discusses the various Program Management challenges presented by Web 2.0 (technical and non-technical). The challenges are categorized into eight major areas: cost, schedule, performance, technologies, process, people, quality and security. In addition to the identified challenges, Lessons Learned and Best Practices are presented to better assist Program Managers in implementing, directing and controlling the various aspects of Web 2.0 that exist within their unique programs, or that exist externally, as their program interfaces with those Web components. Information came from detailed discussions with Web Managers and operational personnel who are intimate with the technical and non-technical aspects of Web 2.0 and the diverse challenges Program Managers have experienced or will engage. This education, awareness, training and knowledge will allow Program Mangers to better manage and solve Web 2.0 issues, today and in the future. Additionally, the DoD decision to restrict access to Web 2.0 social media Web sites is expected in 2010.

14. SUBJECT TERMS Web, Web 2.0, Internet, Information Age, Program Management, Program Manager, programmatic.			**15. NUMBER OF PAGES** 127
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

THE PROGRAM MANAGEMENT CHALLENGES OF WEB 2.0

Yonghee K. Woodall
YD-2, United States Army
B.S., Computer Science, University of Arizona, 2003
M.S., Information Technology, Western International University, 2005

Submitted in partial fulfillment of the requirements for the degree of

MASTER OF PROGRAM MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
June 2010

Author: _____
Yonghee K. Woodall

Approved by: _____
Professor Brad R. Naegle, Lead Advisor

_____
Professor Michael Boudreau, Support Advisor

_____
William R. Gates, Dean
Graduate School of Business and Public Policy

THIS PAGE INTENTIONALLY LEFT BLANK

THE PROGRAM MANAGEMENTCHALLENGES OF WEB 2.0

ABSTRACT

In this Joint Applied Project, the author discusses the various Program Management challenges presented by Web 2.0 (technical and non-technical). The challenges are categorized into eight major areas: cost, schedule, performance, technologies, process, people, quality and security. In addition to the identified challenges, Lessons Learned and Best Practices are presented to better assist Program Managers in implementing, directing and controlling the various aspects of Web 2.0 that exist within their unique programs, or that exist externally as their program interfaces with those Web components. Information came from detailed discussions with Web Managers and operational personnel who are intimate with the technical and non-technical aspects of Web 2.0 and the diverse challenges Program Managers have experienced or will engage. This education, awareness, training and knowledge will allow Program Mangers to better manage and solve Web 2.0 issues, today and in the future. Additionally, the DoD decision to restrict access to Web 2.0 social media Web sites is expected in 2010.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ASD NII	Assistant Secretary of Defense for National Information Infrastructure
CERN	European Organization for Nuclear Research
CIANA	Confidentiality, Integrity, Availability, Non-repudiation, and Authentication
COP	Common Operational Picture
DARPA	Defense Advanced Research Project Agency
DIACAP	Defense Information Assurance Certification and Accreditation Process
DiD	Defense in Depth
DoD	Department of Defense
FTP	File Transfer Protocol
GIG	Global Information Grid
HTML	Hypertext Markup Language
IA	Information Assurance
IO	Information Operations
IT	Information Technology
IW	Information Warfare
JAP	Joint Applied Project
LAN	Local Area Network
MDA	Mission Decomposition Analysis
NIST	National Institute of Standards
NSA	National Security Agency
SANS	Systems Administration and Network Security
SMTP	Simple Mail Transfer Protocol
SOP	Standard Operating Procedures
TAFIM	Technical Architecture Framework for Information Management
TCP/IP	Transmission Control Protocol/Internet Protocol
URL	Uniform Resource Locator
WAN	Wide Area Network
WWW	World Wide Web
XML	eXtensible Markup Language

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

The author would like to thank the advisors, Professor Brad Naegle and Professor Michael Boudreau, for their guidance and commitment in completing this Joint Applied Project. I also would like to express gratitude to my office associates, Ms. Carol Lewis and Mr. David Jones for their patience, understanding, and encouragement through the period of this project.

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Program Managers face many daily challenges, but none as challenging as the newly emerging technologies they must evaluate for incorporation within their programs. Given the rise of the Internet and the pervasive use of Web technologies in today's Information Age, it is imperative for a Program Manager to understand these Web technologies, how they are evolving, and how best to select product implementations that might enhance their program's current and future capabilities. To do otherwise would jeopardize their program's overall effectiveness, quality and efficiency. But choosing the appropriate Web technologies to employ is a major challenge in itself. There are many fast changing trends in the use of World Wide Web technology that enhance creativity, information sharing, collaboration and functionality. Since this is basically pioneering territory for everyone, there are no definitive experts. No one knows what the future holds for network-centric materiel development. We are in the early stages of the Information Age and Program Managers must embrace it and the Web. Today's Web is primarily Web 2.0 based.

Although these Web technologies are indeed new, they bring with them traditional challenges the Program Manager can start to assess based upon their past experience: cost, schedule, performance, technologies, processes, people, quality, and security issues. Complicating this are the many iterations of Web technologies termed "Web Version x" that pop up (aka Web generations). The most prevalent Web technology (generation) today is Web 2.0 but others are evolving too (Web 3.0 and 4.0). Web 2.0 concepts have led to the development and evolution of online Web-based communities and services such as auction houses, knowledge portals, social networking sites, video or music sharing sites, wikis, blogs, and chat rooms, etc. Capabilities provided by these Web implementations provide tremendous synergy to all our activities, saving resources and promoting speedy communications within a network-centric global environment. They are crucial to achieving Information Superiority within our operational environments. Program Managers must rise to the Web challenge, especially those new challenges present with Web 2.0 and its future generations.

The scope of the JAP research was limited to Web 2.0, its immediate future, and its current environments (military, federal and commercial). Emphasis was on Web 2.0 in a military environment, primarily the U.S. Army. During the period 1 October 2008 to 30 November 2009, the author researched Web 2.0 and identified its many challenges.

Significant Findings: Many debate the existence of Web 2.0 and Web generations in general. Regardless of the controversy, many more perceive that Web 2.0 does exist and is in heavy, innovative use. Web 2.0 is mostly a read and write Web environment with limited execute; one that is characterized by social media, social networking, feedback, mutual problem solving, global collaborations and information sharing. Its most remarkable feature is the immense synergy it brings to any mission or business endeavor: Command & Control, teamwork, problem solving, or information dissemination, etc. Individual users are empowered to input or modify Web online or offline content, or to collaborate in a team framework to accomplish mutual goals and objectives. This can be good or bad. DoD is currently deciding to restrict access to social media Web sites. The Marine Corps has already restricted access. The DoD Web 2.0 policy decision is expected in 2010.

Conclusions: Web 2.0 does exist and is here to stay. It is the main enabler of the Information Age aside from people. Web 2.0 is today's Web generation, and it can be defined and its training engaged. It offers many daunting challenges. No official definition or baseline of Web 2.0 exists. The best unofficial Web 2.0 definition is on Wikipedia at http://en.wikipedia.org/wiki/Web_2.0. Wikipedia is itself a Web 2.0 expert technology and a worldwide recognized knowledge center.

Recommendations: Employ Web 2.0 with prior approval and in a secure manner. Train on and use Web 2.0 within its policy parameters. Stay within Command guidance, security, Certification and Accreditation policy requirements. Address Web 2.0 challenges early: cost, schedule, performance, technology, process, people, security and quality. Monitor the known Web 2.0 technologies and those evolving (e.g., Web 3.0 and 4.0); have a Web 2.0 Management Plan. The assured use of the Web is key to DoD Information Superiority. Much synergy and productivity can be gained provided the Web is used and managed responsibly. Program Managers must rise to the cause.

I. INTRODUCTION

A. RESEARCH INTRODUCTION AND SCOPE

Program Managers face many daily challenges, including the substantial challenges introduced by newly emerging technologies that must be evaluated for incorporation within their programs. Given the rise of the Internet and the pervasive use of Web technologies in today's Information Age, it is imperative for a Program Manager to understand these Web technologies, how they are evolving, and how best to select product implementations that might enhance their program's current and future capabilities. To do otherwise would jeopardize their program's overall effectiveness, quality and efficiency. But choosing the appropriate Web technologies to employ is a major challenge in itself. There are many fast changing trends in the use of World Wide Web technology that enhance creativity, information sharing, collaboration and functionality. Since this is basically pioneering territory for everyone, there are no definitive experts and no one knows what the future holds for network-centric materiel development. We are in the early stages of the Information Age and Program Managers must embrace it and the Web.

Although these Web technologies are indeed new, they bring with them traditional challenges the Program Manager can start to assess based upon their past experience: cost, schedule, performance, technologies, processes, people, quality, and security issues. Complicating this evaluation are the many iterations of Web technologies termed "Web Version x" that pop up. The most prevalent Web generation (technology) today is Web 2.0. Web 2.0 concepts have led to the development and evolution of online Web-based communities and services such as auction houses, knowledge portals, social networking sites, video sharing sites, wikis, blogs, and chat rooms, etc. Capabilities provided by these Web implementations provide tremendous synergy to all Web-based activities, saving resources and promoting speedy communications within a network-centric, global environment. They are crucial to achieving Information Superiority within our operational environments. Program Managers must rise to the Web challenge, especially those challenges present today with Web 2.0.

The scope of the research was limited to Web 2.0, its immediate future, and its current environments (military, Federal and commercial). Emphasis was on Web 2.0 in a military environment. During the period 1 October 2008 to 30 November 2009, the Author researched Web 2.0 and its associated challenges. The Author analyzed specific implementations of Web 2.0 as it pertains to the United States Army architectural framework and related its challenges to the various military services, the Army Materiel Command's Chief Information Office/G-6, (CIO/G-6) and to their Special Projects Office (SPO).

B. RESEARCH PURPOSE

The purpose of this research is to gain a basic understanding of Web 2.0 and its many technical and non-technical challenges. Identify those Web 2.0 challenges the Program Managers must solve within their individual program or the challenges they might face when they integrate their program into a system-of-systems or within the Global Information Grid (GIG) network where Web technologies are prevalent.

1. Goals

This project examined the technical issues and non-technical aspects (programmatic and financial) of Web 2.0 to determine the challenges it might present Program Managers today and in the future. These challenges relate to cost, schedule, performance, technologies, process, people, quality, and security. Web technical issues were identified and examined as a basis to discover relevant technical challenges (hardware, software and network). Discussions with Web managers, Program Managers and operational personnel identified technical and non-technical aspects of Web 2.0 that present challenges to Program Managers who must implement and evolve this capability. Additionally, Web 2.0 Lessons Learned, Best Practices, and future were explored. As a result of this project, Program Managers will better understand Web 2.0 and it various challenges, solutions, Lessons Learned, and Best Practices. Research goals included:

- Gain a basic understanding on Web 2.0, its concept and technologies.
- Identify Web 2.0 challenges (issues), especially those that relate to Program Management.

- Identify Web 2.0 Lessons Learned and Best Practices.
- Identify the future direction Web 2.0 might take.

2. Objectives

To determine the current and future, technical and non-technical challenges that Web 2.0 might present Program Managers based upon answers to the following questions:

- Q1: What is the definition of Web 2.0?
- Q2: What were the characteristics of the predecessors to Web 2.0?
- Q3: Where do Web 2.0 implementations exist today?
- Q4: What are the benefits of Web 2.0?
- Q5: What are the issues surrounding Web 2.0?
- Q6: What are the Web 2.0 Lessons Learned and Best Practices?
- Q7: What is the future for Web 2.0?

C. RESEARCH METHODS

Research was based upon past Best Practices research standards normally found within industry, the military, and at the Naval Post graduate School. Past Lessons Learned from previous research efforts were employed to enhance this effort.

1. Methods

Research methods employed consisted of both Quantitative and Qualitative professional methods (i.e., a mixed-methods research). The Quantitative method was a systematic scientific investigation into Web 2.0 with a focus on objective data; especially datum that could be measured and displayed (e.g., numbers, statistics, percentages, tables, graphs, and models, etc.). The Qualitative method was exploratory in nature using observation, interviews, surveys, questionnaires, expert opinion, online Internet searches, and relied on subjective data across multiple disciplines (cost, schedule, performance, technologies, process, people, quality and security, etc.). Researched areas included these environments:

- Private and public sectors.
- Military (Army, Navy, Air Force and Marine Corps).
- Federal.

2. Data Types and Sources

Numeric, alpha numeric, and textual unclassified data was collected, reduced and categorized. It was analyzed to determine what likely program management challenges Web 2.0 presents.

Data was collected from commercial, Federal, and military (Army/Navy) Web sites, and the Program Management offices related to those Web sites. Data included cost, schedule, performance, technology, process, people, quality or security oriented information. Additional data was collected from other military services for comparative purposes (e.g., NPS). The research used methods that were both Quantitative and Qualitative, and presented objective and subjective unclassified data (technical and non-technical).

Data sources will included observation, interviews, literature review, Internet searches, surveys, questionnaires, subject matter expert opinion, vendor brochures, and the Web technologies themselves (e.g., YouTube) from both the military, private, and public sectors. This data was collected from Web sites, Program Management Offices, vendors, experts, and elsewhere as pertinent to the research.

3. Data Collection

A data collection strategy based upon Best Practices collection methodologies and Lessons Learned from previous efforts was employed. Six Sigma guidelines were used as appropriate. The primary data collector was the Author; however, others assisted as assigned (e.g., Author's local and NPS advisors).

Data collection instruments were literature or vendor printouts, surveys, questionnaire forms, interview forms, Internet search result printouts, milestone or project charts, notes, and other instruments as appropriate to the research (e.g., created during the research based upon research discoveries at that time).

Datum collected was grouped into their respective data type category within their respective analysis category (e.g., cost, schedule, performance, technical, process, people, quality, and security).

D. RESEARCH DELIVERABLES

The primary deliverable for the research is the Joint Applied Project (JAP) itself (a Professional Report). It contains an analysis sufficient to determine general and specific Program Management challenges of Web 2.0 (technical and non-technical). The report provides information sufficient to provide a basic Web 2.0 understanding, its challenges and potential solutions, and the presentation of any discovered Lessons Learned and Best Practices. Report includes findings, conclusions and recommendations as well.

The report provides "answers" to the JAP Objectives: To determine the current and future, technical and non-technical challenges that Web 2.0 might present Program Managers based upon answers to its designated questions (Sub section 2: Objective under Section C: RESEARCH PURPOSE).

E. JOINT APPLIED PROJECT ORGANIZATION

JAP organization takes an initial, high level approach to the topic of Web 2.0. It presents an introduction to the topic and provides a detailed background to set the context for understanding the challenges of Web 2.0. A good understanding of the Information Age and the Internet, and their chief enabler (the Web) sets the stage for a deeper analysis of Web 2.0 itself. Due to ambiguity on the standardized definition and architecture of Web 2.0, discussions centered on Web 2.0 products and capabilities to demonstrate its use, misuse, and its challenges. Subject Matter Experts, managers and operational personnel at various Web sites were contacted to gain their insight into Web 2.0 with emphasis on its challenges. Data related to those challenges were collected, analyzed and findings reported in this JAP. Detailed JAP organization is depicted within the report Table of Contents.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND

A. INFORMATION AGE OVERVIEW

To best understand Web 2.0 requires a thorough understanding of its history and evolution over time, to include why and how it initially came about. To do this, a detailed review of the Information Age, the Internet and the Web are paramount. From this foundation, this research can better explain the technical and non-technical aspects of Web 2.0, and the reader can better understand the overall context of the Web 2.0 framework and the dynamic changes that are occurring within it daily. Emphasis within this JAP is on the United States military perspective (Army).

1. Definition of Information Age

The time people live in today is like no other time. Everything is networked via computers: homes, schools, libraries, stores, and businesses. People do not have to go to physical buildings to get educated, research a topic, buy goods, or do work. In the Information Age, people are not limited by physical boundaries or time. Virtual worlds (Communities of Interest such as Chat Rooms) are all around; people can get almost any information anytime, and anywhere. This is the new age people live in; one rich in information and communication technologies.

Having and using “information” has always been the basis for power throughout human history, whether in the cave man days or today. Knowledge is power. In the new Information Age, information is now much more valuable and powerful than other physical things we've seen in the Industrial Age.

The easy and fast access to information with new technology has transformed people’s daily lives and affected every facet of the environment. People have become increasingly dependent on the information and its infrastructures (hosts and networks) to provide or receive accurate and timely distribution of information for decision making. This dramatic change presents many diverse challenges and everyone has a different view about the Information Age since it is so new and not yet well understood. So, what is this Information Age?

The interpretation of the Information Age is different among different groups. The International Technology Education Association (ITEA) defines the Information Age as follows:

> A period of activity starting in the 1950s and continuing today in which the gathering, manipulation, classification, storage, and retrieval of information is central to the workings of society. Information is presented in various forms to a large population of the world through the use of machines, such as computers, facsimile machines, copiers, and CD-ROMs disks. The Information Age was enhanced by the development of the Internet; an electronic means to exchange information in short periods of time, often instantaneously. (ITEA Glossary site, 2009, para 1)

An online dictionary site, TheFreeDictionary.Com, provided yet another definition of the Information Age: "A period beginning in the last quarter of the 20th century when information became easily accessible through publications and through the manipulation of information by computers and computer networks" ("Information Age," n.d.).

The United States Army has its own definition, too:

> The future time period when social, cultural, and economic patterns will reflect the decentralized, nonhierarchical flow of information; contrast this to the more centralized, hierarchical, social, cultural, and economic patterns that reflect the Industrial Age's mechanization of production systems. (DOD, 1996, U.S. Army Field Manual 100-6, Information Operations [IO])

The Department of Defense (DoD) has put its own Information Age doctrine into its Joint Vision publications 2010 and 2020 to better assist the military in understanding it.

Although these definitions seem slightly different, they really are about the same thing and have one thing in common: decentralized operations on "information" utilizing computers, their software, and the wired and wireless networks. As discussed so far, the Information age has had a profound affect throughout society. People are interested in having access to its vast network (the Internet) and information, being mobile, and collaborating with people worldwide. They are purchasing cellular phones or personal digital assistants, and networking their schools. Businesses are transforming into

e-commerce and they are globalizing to the world markets. Outside of business, people also see the rapid growth of distant learning and tele-medicine. It is still difficult to foresee the full breadth and depth, and impacts of the Information Age on society but no doubt, the Information Age will continuously change society. The Information Age is in its early stages and here to stay. It is best to gain an immediate education on it and leverage its many capabilities and advantages to become "information haves," versus being left behind as "information have nots."

Information Age Noteworthy Facts

- The Information Age is here to stay. It will evolve at a fast pace.
- The networking of computers is allowing easy access to information in the Information Age (network centric access to information on a global scale upon demand).
- Information and Knowledge are the basis for power and success. Today's automated enablers allow people to share information more rapidly and to identify and access required information in a rapid fashion (shorter decision cycles than adversaries).
- The Information Age provides a global "equalizing" currency, which is "information" itself. Information within the Information Age is comparable to green-back dollar accumulation during the Industrial Age to become rich. Today the accumulation of "information" makes one Information Age rich.
- The future medium for transport of information (Web networks) shall evolve to be predominantly wireless based. However, a hybrid framework of cables and wireless means will still exist.
- In the Information Age, via Web pages or blogs, etc., people can express their viewpoint(s) without the censorship of any central authority. They are free to provide accurate or inaccurate information or personal opinions

at will. They can interact dynamically on a "one to one" basis in many social sessions, official and unofficial.

- In the Information Age as people use more information technologies there is an increased trend in cyber intrusions and a critical need for better online and offline security.

People are living in a period when information access and quality are critical, much more important than it has ever been. Innovative uses of information can make or break people (personally or as a nation). How people operate on information will determine success or failure and whether their military wins or loses a war. But what are Information Operations?

Information Operations

As discussed in the above Information Age section, information is critical in the Information Age (especially to decision-making and assured mission / business process success). How should people operate on critical information in a manner that increases mission / business process effectiveness, efficiency and security? There is no single strategy that might achieve these goals over time. DoD has derived its own interpretation of what the Information Age means to it. They expressed their concept on it in Joint Chiefs of Staff Publication 3–13, the 1998 document that captured their Doctrine for IO, and within their capstone documents entitled Joint Vision 2010 and 2020. Those documents identified DoD's IO objectives and provided general guidelines concerning IO planning and conduct within the Information Age.

DoD defined IO as "Actions taken to affect adversary information and information systems while defending one's own information and information systems (DoD IO Joint Publication 3–13, 1998, p. I–9)." IO actions contain many different activities that include human and automated information based processing. Figure 1 illustrates many different IO capabilities and related activities for building IO. It includes Information security, public affairs, physical security, communications security, deception, computer security, physical attack / destruction, counter intelligence, counter-

propaganda, network management, electronic Warfare, operations security, computer security, computer network attack, civil affairs, and others. It is easy to see that IO are in everything people do.

Figure 1. Information Operations: Capabilities and Related Activities
(From Joint Pub 3–13, 1998, p. I–10)

IO can be divided into two major parts: Offensive IO, which is synonymous with Information Warfare (IW), and defensive IO, which is synonymous with IA (DoD IO Joint Pub 3–13, 1998).

Outside of the DoD within the private, local governmental and industrial sectors, IO has an emphasis on business "processes." IO has been publicly studied and publications exist that elaborate on those processes (mostly at the academic level). Within the public domain, some Information Age and IO terms and definitions are similar to DoD's, while some are different. Most noteworthy within the public domain are the past studies into functional process improvement, business process re-engineering, and quality initiatives (e.g., Baldridge, Total Quality Management, International Standards Organization 9000, Six Sigma, and Lean Thinking, at http://www.isixsigma.com/me/).

These past initiatives did not necessarily focus on the Information Age or on automated IO, but still they possess information related to the processing of assured and secure information within formal business process constructs. After all, Information Assurance (IA) is assured IO.

Within the Federal arena, under the Department of Commerce, the National Institute of Standards (NIST) has researched and published numerous documents within its Computer Security Resource Center that pertain to cyberspace, with some targeting network security and intrusions (http://csrc.nist.gov/publications/nistpubs/index.html). NIST's main focus for IO is securing traditional business processes, information systems, and networks within industry at the public and federal level.

To better understand IO and the related processes that use information as a resource, people must first take a "big picture" look at an organization's overall mission or business architecture and decompose it into its subordinate missions, functions and tasks to discover its critical information objects and their related critical infrastructures, and the "high risk" operational threads (process paths) that share information up and down that architecture (horizontal and vertical information sharing). This process is called Mission Decomposition Analysis (MDA).

Generic high-level IO processes are based on the traditional Information Model, a system view that includes input, processing, output and storage. The processing stage can add, delete or modify data. In reality at lower levels, the IO processes are processes to manipulate information or support the operations on information (i.e., IO).

Within DoD and in the Joint Vision doctrine, these IO processes fall under major "Information Age" -type IO processes (also called tenets in a different context): Information Superiority, Full Spectrum Dominance, Focused Logistics, Full Dimensional Protection, Dominant Maneuver, Precision Engagement, and Decision Superiority (Joint Chief of Staff, 1997).

Each IO process operates on a given piece(s) of information, an "information object." The term "information object" was first used in an old 1990s DoD architectural document, the Technical Architecture Framework for Information Management

(TAFIM). The concept of information objects allows one to focus on information itself "logically" as an object of varying size (i.e., an Information Age-type concept). Within the Industrial Age, physical products could be small (pencil) or large (airplane) in size. Within the Information Age, its logical products might be small (e.g., a single number such as "6") or large (e.g., DoD "enterprise report" to Congress on the status of Equal Opportunity within all the military Services) also. Likewise, an online social group or a Web technology could also be viewed as an information object.

The purpose of identifying "logical" information objects allows the ability to identify their physical locations (i.e., their infrastructure component identification such as their residing on a diskette or a server hard drive), and many other useful pieces of information. Examples (not all inclusive): 1) The value of that single information object in relation to other information objects (its importance, its criticality to the overall mission or business, and what operational thread it supports); 2) The security on that physical location (hence the security on that information object and that security within its related mission / business process operational thread); and 3) The age (time stamp) of its information (current or outdated data). Information objects can have diverse value over time, and with respect to the provider or consumer of that information.

The aggregation of all these information objects provides great insight into their overall infrastructure understanding (i.e., their infostructure). It also facilitates the identification of high risk operational threads within critical missions that might need greater security. Security is at a lower level as depicted in Figure 2 (a subset of IA). This also allows decision makers the insight to know which information objects require greater protection and defense from intrusions (based upon their criticality and the physical infrastructure they reside on). Depicted below is a representative decomposition process (example structure). The cognitive ability to deal with these types of abstract concepts in the Information Age is invaluable; as "information" is a logical concept, and very abstract and difficult for most people to grasp. Likewise, the online discussion of information in Web forums presents a tremendous managerial and security challenge. These information objects are transported by both wired and wireless networks over the Internet using today's Web technologies (HTML browsers, etc.).

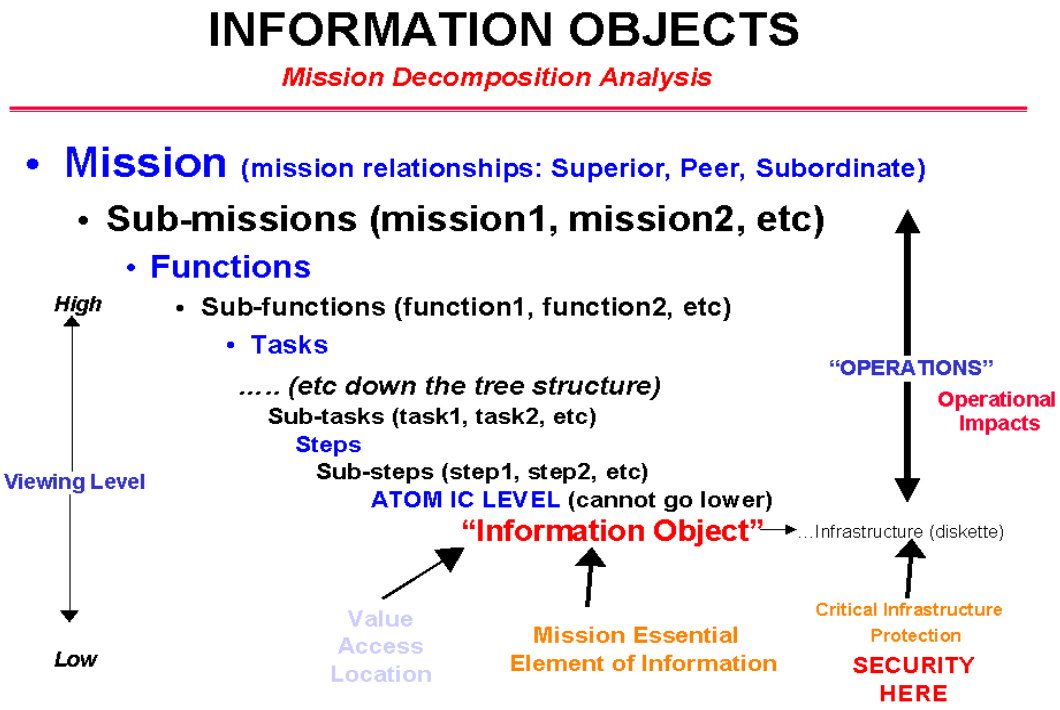


Figure 2. Mission Decomposition Analysis to Identify Information Objects.

Knowing the "how, when and where" as the information objects are transported across the networks (or processed by hosts or Web servers) is very important, especially for managers controlling security or hackers seeking to access them. Without proper protection (encryption), the wired or wireless networks might pass their information "in the clear" for all people to see. Access control requires encryption and authentication. Thus security is a major challenge for all, especially those using the Web.

Key information related to IO

- The Information Age (and IO) is here to stay so people must understand and embrace it (especially its abstract IO concepts). Cognitive abilities are a must.
- The definition of IO is not mature or well understood (same for information objects and assigning them value and access controls, and the evolving Web).

- IO does not get managerial attention and emphasis to ensure appropriate identification, inventor, and currency. Managers know but are unaware of the physical location and quantity of their computers the logical information objects that reside there, or their localized information object security.
- A significant amount of IO are not institutionalized, written or enforced (e.g., Standard Operating Procedures (SOP) not written or published to ensure consistent standardized operations or monitoring of Web forums).
- The relationship of IO to their higher parent (business or mission process) is not well understood. Traceability (operational threads) is not fully documented from the top down structure of the mission/business to the IO and its related "atomic level" information objects.
- The use of wireless networking will increase risk to assuring and securing IO and its information objects.

Information Architectures (Information Structures)

An Information Infrastructure consists of communication networks, computers, software, applications, databases, Web technologies, and users' electronics (hardware). An Information Infrastructure exists at different levels: global, national, regional, and/or local level, and can possess both technical and non-technical characteristics.

- A few definitions of Information Architecture are provided below. The Information Architecture Institute defined Information Architecture as:
- The structural design of shared information environments.
- The art and science of organizing and labeling Web sites, intranets, online communities and software to support usability and findability (discovery).
- An emerging community of practice focused on bringing principles of design and architecture to the digital environments. (Information Architecture Institute, Information Architecture, para 2).

- The book Information Architecture (2nd Edition) defined Information Architecture as:
- The combination of institutes or groups, classification, and design schemes within an information system.
- Structured information building blocks that facilitate functions, tasks, and activities completion.
- An order and community of practice focused on bringing values of design and architecture to the digital environment (Rosenfeld & Morville, 2002).

The DoD view of architectures is set by the Assistant Secretary of Defense for National Information Infrastructure (ASD NII) http://www.defenselink.mil/cio-nii/ as being three views: technical, system, and operational.

Operational Architecture is the narrative or graphical description of the operational aspects, tasks, and information paths required to sustain the warfighter (DoD Architecture Framework, 2004). Systems Architecture "defines the physical connection, location, and identification of key nodes, circuits, networks, warfighting platforms, etc., and specifies system and component performance parameters. The systems architecture is constructed to satisfy operational architecture requirements per standards defined in the technical architecture" (DoD, Architecture Framework, 2004). The systems architecture illustrates how various systems link to each other and may show the internal structure of certain systems. The technical architecture defines the "services, interfaces, standards, and their relationships. It provides the technical guidelines for implementation of systems upon which engineering specifications are based, common building blocks are built, and product lines are developed." (DoD, Architecture Framework, 2004). DoD has charged the National Security Agency (NSA) to develop their Enterprise IA architecture to ensure DoD-wide protection and defense. DoD views this area as critical to assuring their overall operational mission. The private sector and industry have similar architectural concepts and depictions (graphics / diagrams) to DoD, since most were developed via mutual collaborations using the new Web technologies.

An Information Structure is a notional concept. This infostructure is a means to hierarchically place "logical" (non-physical) information objects of varying size, value or importance in some structured relationship (e.g., table or diagram) within cyberspace on the Web. This provides a better understanding on how they relate to each other from an Information Model (input, output, processing and storage), processing, and a military / business process perspective. This structure facilitates many views into the mission / business processes, from large to small, and allows the ability to identify and trace operational threads from top to bottom within that structure.

Knowing what is critical (important) allows the ability to determine within that infostructure the critical physical infrastructure that requires the greatest protection and defense (or resource expenditures). From a network centric perspective, architectures are used to diagram the various networks that support the infrastructure to provide a basis to better understand their technical connectivity and security. This is especially true for understanding the Web technologies. Architecture helps to better understand the Web boundaries, horizontally and vertically, as they exist out on the various global networks.

Information Architecture noteworthy facts

- An understanding of the mission / business processes (architecture, infostructure and information object flow) must exist. Knowing what the business is (its overarching vision, goals and objectives) is critical to eventual success (what is important to share on the Web, and to protect and defend).
- Architectural strengths and weaknesses must be documented and Web component vulnerabilities addressed and mitigated.
- Intrusion prevention and detection cannot be performed in a vacuum. To be truly effective and efficient, it must be well thought out within the overall context of the mission / business processes (IO) to be performed (its architecture), while knowing what specific IO, operational; threads, information objects, and infrastructures are most important to protect and

defend first. Understanding people and their online social interactions, official business and unofficial, are critical to maintaining good security.

- Wireless technologies are a great challenge as its radio waves permeate the whole organization and its infrastructure, with the potential to touch all information objects, their IO, and the Web. Worldwide interaction is possible.

Information Assurance

"IA is Information Operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non- repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities" (DODD 8500.1, 2002, p. 20).

What is IA really? It is not security alone although security is included and very important. IA is a much broader topic and includes Enterprise-wide protection and defense across all technologies, processes, and people within the DoD Global Information Grid (GiG) network (especially the Web components). Employing IA in a comprehensive manner assures DoD successful mission execution, and promotes Joint Vision goal achievements (Information Superiority, Full Spectrum Dominance, and Full Dimensional Protection, etc.). "IA is the component of Information Operations that assures DoD's operational readiness by providing for the continuous security, availability, and reliability of information systems and networks" (IWS, ASDNII CIO FAQ, The Information Warfare Site, para 23).

To facilitate understanding and enforcement of IA, DoD publishes and inspects these attributes associated with their networked Information Technology (IT) assets:

- Their Protect, Detect, React, and Recovery (security) status.
- Their Confidentiality, Integrity, Availability, Non-repudiation, and Authentication (CIANA) information security characteristics.

- The certification and accreditation of the various IT components (i.e., Defense Information Assurance Certification and Accreditation Process (DIACAP)). Testing IT components prior to use is a Best Practice, especially those components to be use within the online Web environments.
- The Networthiness and Netreadiness of IT components prior to connection and their operational status after connection. The Webs we create and operate must be secured and assured at all times.

Within the last few years, DoD has expanded its IA concept and capabilities to encompass more than technical security. They now include non-technical security, and focus on a more comprehensive network centric view that dictates they assure and secure all technologies, processes and people within their architectures / infostructures over time (hence assure everything). Unfortunately, limited budgets and the current wars constrain this desire. Scarce resources applied to the Web must be carefully managed.

The public civilian view about IA centers mostly on its security functionality and characteristics. Within the civilian community there are comparable approaches to DoD's IT security and intrusion detection. The IA training provided by the Systems Administration and Network Security (SANS) organization has been instrumental in this common base of knowledge. Within academic arenas, studies also indicate that IA is much more than security alone, that it involves assured and secure technologies, processes and people over time. Within Web environments, this is now critical.

A Best Practice in IA is to use only tested products and services that actually work and do not degrade security. Deeming items "worthy" is Networthiness. Networthiness is an initiative to investigate the worthiness of an IT component (e.g., a Web component) to be connected to an established network (a Best Practice and operating concept). This usually involves a technical test, and an assessment of its processes and personnel support requirements, to ensure it is well understood before connection. Areas of consideration: IA, its technologies, processes, people, and any issues it might present to the environment where it might be employed (interoperability,

conflicts and competition over resources). Once it has been tested and a recommendation made to employ it (certification), owners of the intended operating environment make informed decisions on whether to use it (accreditation). They consider all its known characteristics and determine if it is worthy to join their current IT suite and whether it will enhance or degrade their overall mission / business processes and security posture. This Networthiness must be applied to the various Web technologies as well as its online Web forums that pass on information. A Lesson Learned is to test, certify and accredit Web and network components before their actual connection.

To better understand what people are to secure, or why they have to assure anything, requires an understanding of the various threats posed to operating environments. Typically these threats fall into these eight categories (priority order top down): natural disasters, power, mis-configured equipment, poorly trained employees (accidents or low skill), disgruntled employees (malicious), malware (poorly programmed Web code, virus, Trojan and worms), Hackers, and miscellaneous unexplained events (disruptions to technologies, processes and people). Most view trusted insiders as the greatest threat.

It is also a Best Practice to routinely identify commonly known vulnerabilities and exposures and to mitigate them before they occur. Mitre Corporation chose to categorize all the commonly known vulnerabilities and exposures in a classification database at http://www.cve.mitre.org/. As of 11 March 2009, there were 35,548 commonly known vulnerabilities and exposures that might be exploited. The unfortunate truth is the threat changes daily (hourly) and may be technical and non-technical in nature, varying over time. The proliferation and openness of the Web and its many new uses (e.g., Twitter) really increases this risk.

IA noteworthy facts

- IA is more than security alone. It involves secure and assured technologies, processes, and people over time.
- IA is a huge and complex topic. Few really understand it and its challenges.

- Proper IA is a collaborative enterprise and global effort to be successful.
- An important aspect of both security and IA is understanding and dynamically reacting to threat (intrusions)—prevention and detection assist in this endeavor.
- Intrusions can never be 100% prevented or detected given the current state of technology, poor understanding of IA, and the human element within our protection and defense.

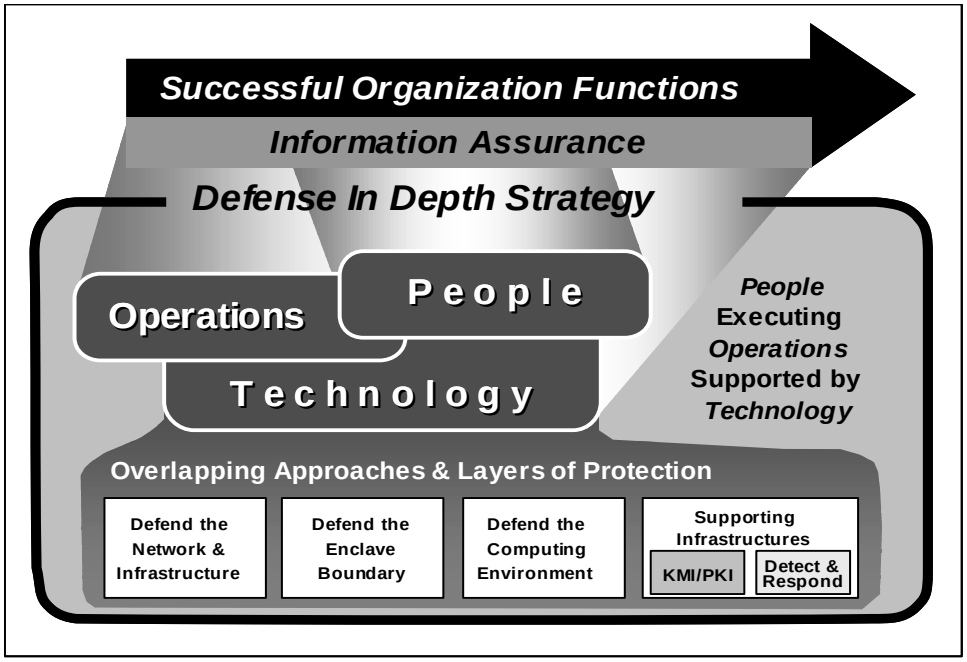
Defense in Depth (Protection and Defense)

As the term suggests, Defense in Depth (DiD) is a set of multiple security solutions, both technical and non-technical that act in concert. The best high-level reference for DiD is on the National Security Agency (NSA) Web site in their short DiD tutorial at http://www.nsa.gov/ia/_files/support/defenseindepth.pdf .

- The best approach to DiD is to have a collection of layered security solutions within these three domains: technologies, processes and people. They all must work in concert together to protect and defend the missions / business processes in a given architecture. Varying degrees of these DiD solutions may be applied depending upon what is to be protected, its value, the current threat, and the risk that can be afforded. "Implementation of this approach recognizes that the highly interactive nature of information systems and enclaves within a global world creates a shared risk environment; therefore, the adequate assurance of any single asset is dependent upon the adequate assurance of all interconnecting assets" (NSA IATF V3.1, 2002, Appendix B Glossary).
- The DiD is a "balance" among cost, schedule, and performance that one requires to assure their mission / business processes over time. "It is a practical strategy because it relies on the intelligent application of techniques and technologies that exist today. This strategy recommends a

balance among protection capability, cost, performance, and operational considerations" (NSA IATF V3.1 Chapter 2 DiD, 2002, p. 1).

- The DiD strategy organizes these requirements into four main areas of focus (NSA and DoD type perspective): 1) Defend the Network and Infrastructure, 2) Defend the Enclave Boundary, 3) Defend the Computing Environment, and 4) Supporting Infrastructures as depicted in Figure 3.



- People
  - Policies and Procedures
  - Training and Awareness
  - Physical security
  - Personnel security
  - System security administration
  - Facilities Countermeasures
- Technology
  - IA Architecture framework areas
  - IA criteria (security, interoperability, and PKI)
  - Acquisition integration of evaluated products
  - System risk assessments
- Operations
  - Security policy
  - Certification and accreditation
  - Readiness assessments
  - Security management
  - Key management
  - Attack sensing and warning response
  - Recovery and reconstitution

Figure 3. Principal Aspects of the Defense-in-Depth

(IATFF Chapter 2, September 2002, p. 2-11)

Thus, DiD is really the employment of multiple security solutions over technologies, processes and people over time (i.e., layered security). Layered security is the combination of security services, software and hardware, infrastructures, and processes which are implemented to achieve a required level of protection. These mechanisms are additive in nature with the minimum protection being provided by the network and infrastructure layers and the human element (especially the trusted inside gone bad), a major issue for DiD).

To better implement DiD, international organizations have tried to establish common standards for developing and testing the vast array of technologies that might be developed to secure hosts and networks (e.g., Common Criteria); however, this Common Criteria effort has declined. Since security products developed to standards may vary from vendor to vendor, it is best to ensure professional Web products integrated into any DiD be effective (hence tested).

DiD noteworthy facts

- An effective DiD must embrace layered security solutions (technologies, processes and people) in a comprehensive manner over time. Update them as new ones emerge.
- The human element within any defense implementation poses the greatest threat. Hence the online Web (e.g., forums) poses a significant challenge.
- Managers will never have enough money or time to implement the DiD solution set that they really must have. Auditing what one "can afford to have" is critical.
- There is no perfect DiD solution set. Contingency and backup planning is crucial.

- Web technologies will need a very rigorous DiD solution set applied to them as they present great risk (threat plus opportunity). Their open architecture and access pose tremendous managerial challenges. Obtaining timely and accurate Web situational assessments (i.e., Common Operational Picture) will be difficult.

Information Assurance Common Operational Picture (IA COP)

The COP is defined as "A single identical display of relevant information shared by more than one command. A common operation picture facilitates collaborative planning and assists all echelons to achieve situational awareness" (DoD 2004, Joint Pub 1-02).

Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3151.01 defined COP as follows: "The Common Operational Picture (COP) is a distributed data processing and exchange environment for developing a dynamic database of objects, allowing each user to filter and contribute to this database, according to the user's area of responsibility and command role" (p. 56).

To better understand the status (health) on the Web requires one to either test and evaluate it (objective activities), or to assess it (subjective activities). Afterwards, the results from that effort can provide insight into the many variables associated with the Web's network, its information and activities. Knowing the COP, one can better understand what is going on internally and externally to that Web implementation from a cost, schedule and performance perspective (i.e., their individual status and health).

Applying the IA COP construct specifically to Web technologies and their networks, allows managers the ability to know their health (status on general operational activity and any anomalous behavior that might occur as they operate). Implementing an IA COP would provide insight into the status on that Web network as it relates to its operations and intrusions. It would also provide insight into identifying those events to assist in their future prevention, or in knowing when to initiate the Incident Handling Team to counter and contain an intrusion.

IA COP noteworthy facts

- It is costly to effect 100% Web monitoring and intrusion detection (IA COP). Most organizations can not afford it so they must compromise on what they can do, based upon their budget and their business and mission requirements.
- To effect 100% Web monitoring and intrusion detection consumes too much time (impossible to do in a timely fashion or at all due to data volume). Organizations must compromise on what they can do in time allocated, based upon their budget and their business, project, and mission requirements.
- It is impossible to implement an IA COP that prevents, identifies or detects 100% of the events that might occur within a given Web's wired or wireless network. However, an IA COP must be implemented to gain whatever value (%) it might provide. Intrusions and the damage they might inflict must be countered.
- Past and present implementations of Web technologies have little IA COP support mechanisms. It is a Lesson Learned to have a good monitoring and detection capability on all Web networks, especially with a focus on the discrete Web components. The legal aspects of monitoring private individuals on the Web must be fully considered as it might be illegal at times. And the Web on the Internet is huge, stretching globally outside your domain.

2. Definition of the Internet

The FreeDictionary by Farlex (March 20, 2009) defined the Internet as the following:

> A system connecting computers around the world using TCP/IP, which stands for Transmission Control Protocol/Internet Protocol, a set of standards for transmitting and receiving digital data. The Internet consists primarily of the collection of billions of interconnected Web pages that are transferred using

> HTTP (Hypertext Transfer Protocol), and is collectively known as the World Wide Web. The Internet also uses FTP (File Transfer Protocol) to transfer files, and SMTP (Simple Mail Transfer Protocol) to transfer e-mail (para 3).

Today people think of the Information Age in terms of its many uses and devices: handheld computers, cell phones, blackberries, digital music / video, television on demand, search engines, digital cameras, e-mail, gaming, Web surfing, and other new products and services that have come into use (i.e., chat rooms and social forums). These new technologies are effecting vast changes within our society on a global scale. New capabilities are evolving almost daily as new uses of current technologies are discovered (e.g., Twitter). However, what would the Information Age be without some data communication method to share and exchange its information, products and services? Fortunately, we have world-wide networks interconnected across many countries and domains to provide an immense storage, processing and transportation system for our information. We call this network of networks the Internet. But it was not always so.

Automated computers and their networks are relatively new to this century, especially as they exist and are used today. It was not too long ago that the Defense Advanced Research Project Agency (DARPA) created the first small packet-switched network in 1969 to support simple file transfer between two computer nodes. From this small two-node Local Area Network (LAN) we later evolved other LANs with more computers into Wide Area Networks (WAN), and finally into a global grid system of open architecture networks that we now call the Internet (1985). The primary communications protocol for these networks was later evolved in the 1960s–1970s: Internet Protocol Suite (aka Transmission Control Protocol / Internet Protocol [TCP/IP]). Within the military, this complex arrangement of networks is now called the Global Information Grid (GiG), and has both unclassified and classified networks.

> The GiG is the globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GiG includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associate services and National Security Systems. The GiG also includes the unclassified Internet as one of its networks. (DTIC, 2009, para 1)

The Internet Society maintains a detailed history of the Internet at http://www.isoc.org/internet/history/ along with documents that further define the Internet in greater detail. In-depth historical information is also at the "Living Internet" Web site at http://www.livinginternet.com/. Reading its history relates its use by the Web.

B. WEB TECHNOLOGY OVERVIEW

1. Definition of the Web

> "The World Wide Web (known as 'WWW,' 'Web' or 'W3') is the universe of network-accessible information, the embodiment of human knowledge."
>
> (World Wide Web Consortium, 2009, para 1).

The Internet and the Web are not the same. The Internet (1980s) is a global data communications system. It is a hardware and software infrastructure that provides connectivity between diverse computers worldwide using communication protocols. In contrast, the Web (1990s) is only "one of the services" communicated using the Internet and was initiated in the 1990s. The Web is a vast collection of interconnected information, documents and resources (e.g., databases), linked by hyperlinks, and identified by Uniform Resource Locator (URL) addresses. The Web information is usually displayed in Hypertext Markup Language (HTML) Web pages inside a Web browser, or via other methods such as dynamic text / audio / video (multimedia) or eXtensible Markup Language (XML) Web pages. The Web is the online enabler "glue" to tie people to their information on the Internet and to other people within that global environment to share information or to gain synergy through collaborations. Web browsers allow people a viewing area to see and interact with their desired information (or people) from a given computer desktop. There are many redundant paths to online information or to mirror storage areas that contain backups of that information. Given these intricate and overlapping paths to information, the Web is very similar to the common spider web, but in a different "logical" context.

As the Web initially evolved, there was no deliberate attempt or desire to label its various iterations, phases or evolutions. The term Web 0.0 did not exist but there was

definitely a zero iteration of the Web during its creation and infancy, but it was not officially called that. It was not until the early 2000s, did people attempt to categorize the various Web implementations into perceived generations of Web development, design and capabilities (hardware, software, products and services). And even today there is debate on what constitutes each generation (Web technology suite) or if they really exist.

The underlying ideas of the Web can be traced back to 1980 work at the European Organization for Nuclear Research (CERN) in Switzerland, when Sir Tim Berners-Lee laid the foundation for his 1990 project the World Wide Web by writing a proposal for an elaborate information management system. He is also credited with using the first Web server and writing the first Web browser. The limited Web environment he employed was the early stages of Web 0.0 to 1.0, the earliest of Web generations. He is now the Director of the World Wide Web Consortium. The term Web 1.0 came into use after the use of the term Web 2.0 by O'Reilly Media (formerly O'Reilly & Associates) to promote their Web conferences (Web 2.0 Summit). No one deliberately sat and designed Web 1.0 based upon anything in the past or based upon some thought out design. It just happened after people used some of the initial Web capabilities, liked it, and enhanced its many features to support further use. Web 1.0 was mostly the 1992 Internet, browser Mosaic [then Netscape or Internet Explorer], Web servers, and static HTML Web pages. The World Wide Web Consortium maintains a detailed timeline and history of the Web at its Web site http://www.w3.org/History.html. Research within this JAP sought to identify, define and characterize the various Web generations from Web 0.0 up to Web 2.0 and beyond (the terminology), currently in popular usage today. That information is presented later in Chapter III Data.

2. Web Technologies

The online Merriam-Webster Dictionary defines “technology” as “the practical application of knowledge especially in a particular area” (2009, para 2). Thus, a “Web technology” must be the practical application of knowledge within the Web and Internet arenas, and “Web technologies” a collection of these application items.

Many technical and non-technical technologies comprise these Web technologies. From a "technical perspective" these common technologies are predominant: computers, their hardware, software, and networks (wired and wireless, routers, and firewalls, etc). Within the software arena: Web browsers, HTML or XML code, Web pages, Web sites (URL), Web servers, multimedia software, search engines, Bots, protocols, and databases. From a "non-technical perspective" these common technologies are predominant: standards working groups, processes, forums, meetings, collaborations, programming, and personal interactions. JAP research sought to identify the specific Web 2.0 technologies appropriate for Program Manger consideration, and those technologies are elaborated later in Chapter III Data. Many of these technologies are already commonly known (e.g., e-mail) but research revealed many more to include newly emerging ones (Twitter and Mashups, etc.). An inventory of these Web technologies is in Chapter III Data, with insight into their prevalence on the Internet.

C. TRADITIONAL PROGRAM MANAGEMENT CHALLENGES

Since the early years of business or any important initiative, management (or more specific Program Management) has had to identify, deal with, and manage a set of commonly recurring program challenges. These generic "high level" challenges include:

1. Cost, Schedule, and Performance

Whether it was the Agricultural, Industrial or Information Age period, money to fund initiatives to ensure they arrived on schedule with the desired performance characteristics have been the common items to pursue in any management endeavor. No one ever has enough money or time to expend, or the requisite knowledge upfront to know the exact requirements for any given program of its sub-projects. No one is an expert at perfect implementation, and errors or delays do occur. While some of this information is indeed known upfront, as the initiative progresses, they are usually updated as work progresses. It is a Best Practice to have metrics in place to estimate program life cycle cost, funds expenditures (burn rate), schedules and slippages, and

quality of performance to specifications. Likewise, for evaluating Web 2.0 endeavors, metrics must be identified and used to evaluate its cost, schedule and performance within any program or project.

2. Technologies, Process, and People

Within any program endeavor, technologies (technical and non-technical) are employed: material objects (e.g., computers and tools), or broader themes (e.g., systems, organizations, or techniques). People employ these technologies in various processes that support their business, military or personal use. Likewise, for evaluating Web 2.0 endeavors, its technologies, processes and people must be identified and managed for any program or project.

3. Quality

Within any program endeavor, the quality of its products and services is very important (perceptual or real). Components within a Web 2.0 framework must be both effective and efficient, and fully support or military and business operations. Quality measures must be employed to evaluate Web 2.0 success over time.

Security

Within any program endeavor, assured secure success over the various life cycle aspects of the program is critical and must be managed (funds, schedule, performance, technologies, processes, people, quality, and security). Security must be designed in and implemented early in any program's life cycle to assure its information operations, and to protect and defend its critical components. Likewise, security is a prime consideration for Web 2.0, especially given its criticality to mission success and the potential exposure of sensitive or classified information on the Web to those without a need to know. And, since there is no "one perfect security solution," a Best Practice Defense in Depth approach of layered security must be employed for Web 2.0 environments. As Web 2.0 presents newly emerging technologies and evolves to Web 3.0 and beyond, newly

emerging global threats also arise at a rapid pace and they must be countered, to include Trusted Insider issues. New Web technologies must also be assessed before integration to ensure they too are secure and issues known.

Within this JAP, these eight "top level" traditional Web challenges (Cost, Schedule, Performance, Technology, Process, People, Quality, and Security) are further examined to show the specific considerations needed for the general Web, Web 2.0 and beyond. Included are also Lessons Learned and Best Practices to approach these issues and concerns, and hopefully reduce future Program risk. Feedback from operational Web personnel was invaluable. A review of military, business, academia, and public Web sites shows the tremendous diverse collection of Web technologies in play today and evolving. It is one amazing and exciting, challenged-filled Web environment. Program Managers have their work cut out for them as there is much to learn and do. Hopefully, this JAP will assist Program Managers in this endeavor.

THIS PAGE INTENTIONALLY LEFT BLANK

III. DATA

A. DATA OVERVIEW

Data presented within this chapter may be objective or subjective, high level or low level, descriptive or prescriptive, numeric, alpha, or alphanumeric, or be examples of Web 2.0 implementations or devices (hardware, software or networks). Some comments may be speculative, since Web 2.0 is abstract in nature or the information forecasts the future of the general Web or Web 2.0. Specific data related to Web 2.0 Program Management Challenges follows in the below paragraphs. Data presented is not all inclusive to the research study, or to the overall data collection effort performed by the author, but represents significant data relative to the research study as determined from the author's perspective. This was done in the sake of brevity in data presentation. Additionally, raw or very low level Web data is not presented within this chapter, but may be discussed from their aggregate collective level. The author sought to keep only information appropriate to key discussions on Web 2.0 and its ramifications, to avoid reader information overload.

When the author first started this research in October 2008, there was an abundance of discussion and information on Web 2.0 and the other various generations (Web 1.0, 3.0 and 4.0, etc.). But as time passed during 2008–2009 timeframe, there was considerable debate on the Internet indicating that the various Web generations did not really exist, were ill defined, or that they should be integrated into the current World Wide Web (WWW) as just enhancements or continuations of the older Web. Their rationale was that generations (like Web 2.0) were only a continuation of the original World Wide Web (WWW) and its expanding capabilities, and no generation (number) need be specified since there were no clear lines between generations. Thus, discussions regarding Web 2.0 itself did not exist at all, that it, too, was only a continuation of the growing WWW. This widely diverse trend (acceptance and rebuttal of generations and of Web 2.0 itself) affected the author's ability to identify, collect and retain "stabilized data" throughout the year related to Web 2.0 or the other Web generation. It is difficult to collect data on an ill-defined Web 2.0, or generations of that item, when they do not officially exist (i.e., no formal baseline or definitions). However, the heavy usage and innovation occurring on the "old" Web was such that

"something" was indeed out there, in wide use, and rapidly evolving, no matter what it was called (WWW, Web 2.0, Web 3.0 or not). This Information Age growth and Web usage can be viewed as a mere continuation of the original WWW, or viewed to some degree, as discrete generation of that WWW, even if hard to define. Thus, the author collected data from both sides of the controversial discussions: Those that say Web 2.0 (or any generation) does not exist, and those that say generations of the Web (especially Web 2.0) do indeed exist. Regardless of who is right, the operational use of the Web will continue, is in heavy use today, and new innovative ways of using it and sharing information using it shall continue.

The Web is a dynamic entity, expanding daily on a global basis, with an explosion of new innovations, uses and emerging technologies. Unfortunately for the author, research into this topic could not go on forever, and its data collection had to be terminated 1 September 2009 for data analysis and to meet the project submittal due date in early 2010. Besides, debates on Web 2.0 and the generations might continue for several years as it further evolves. Who knows what the future might hold for the Web, its generations, or continuous evolution of a single generation? But the profound impact of the Information Age (and its enabler, the Web) will be with us for a long time to come. Research data sources (not all inclusive):

- Oral Interviews (Program Managers, Webmasters, and Subject Matter Experts, etc.)
- Questionnaires and Surveys (Program Managers, Webmasters, Federal employees, and Subject Matter Experts, etc.)
- Web Forums (Worldwide Web Consortium and Wikipedia Webtalk, etc.)
- Internet (search engines, subscription news feeds, O'Reilly Web 2.0 Conference archives, and Web sites, etc.)
- Books, newspapers, periodicals, white papers, and vendor brochures, etc.
- Personal Web site experimentation (Facebook, MySpace, and Twitter, etc.)
- Government offices (reports and comments from ISEC, GAO and AMC G-6/CIO, etc.)
- Television (e.g., C-Span2 Special on Web 2.0 aired 9 April 2009, titled "Journalism and Social Media," PBS broadcasts and more)

B. WEB 2.0-RELATED DEFINITION DATA

Defining the Web in general terms has many accepted explanations and common agreement on what it means. Usually the term Web means the Worldwide Web (WWW). However, defining the Web into generations titled 0.0, 1.0, 2.0 or 3.0 and beyond is extremely emotional and controversial (i.e., no common agreement). Opinions run the full gamut: the generations do not exist, they are an extension of the commonly known current Web (an enhancement), and on and on, to include specific details on each envisioned generation's capabilities, technologies, and implementations as reality. There is no common agreement on definitions, or whether the various generations actually exist.

Despite its success and rapid spread, the Web is still basically a prototype, an embryo and not mature, but extremely rich in usage and in full operational use. Hence, this research captured several tentative definitions for the various "supposed generations" as depicted below.

Web 0.0 Definition: No official definition exists. Most likely, Web 0.0 was an early Web laboratory experiment at the European Organization for Nuclear Research (CERN) (http://public.web.cern.ch/public/), where Sir Tim Berners-Lee and others tried to transfer or access data files in a more efficient manner using very early Web technologies. This was a period of analog, and analog to digital data connectivity, which was not public to any major degree. Most computer software applications during this period were client-server standalone or proprietary-linked, custom applications. The Internet, as we know it today, was just evolving in 1969 at the Defense Advanced Research Projects Agency (DARPA).

Web 1.0 Definition: As with all of the Web generations, no official definition exists. Most likely Web 1.0 was the first Web implementation deployed outside the experimental labs into the public or military domains. "The term Web 1.0 is used mainly to reference the time before Web 2.0. No one ever called Web 1.0 by this name when it was occurring. **…**Here we will use the term Web 1.0 to label the set of Web-defining technologies in the late 1990s and early 2000s" (Newman & Thomas, 2009, p. 4).

Web 1.0 was basically a "Read Only" online Web environment (the fledgling of what we know today). A Web environment that consisted of initial, low capability browsers (Mosaic) with public, simple Hypertext Markup Language (HTML) Web pages (initially text only pages and later, text with graphics) accessed over telephone dial-up lines or within small internal networks. Web servers and pages existed that supported multi-media in a limited fashion. Most were static Web environments with initial animation and some interface to offline databases (Microsoft Access and Oracle). The early Web grew over the foundation set by the early 1969 DARPA Internet networks based upon the Internet Protocol Suite. This later included the evolution of Intra-nets (internal or private networks).

Web 2.0 Definition(s): While no official definition exists, Web 2.0 is basically a "Read and Write" online Web environment but with rapidly expanding capabilities (i.e., incorporating innovative uses of social media and collaborations). Web 2.0 is a perceived next generation of the Web after Web 1.0; however, many argue that point as previously discussed.

> The notion of Web 2.0 is somewhat problematical: Tim Berners-Lee, who can be described as the founder of the Web, described it as "*a piece of jargon,*" pointing out that blogs, wikis and the technologies of collaboration and interaction are simply manifestations of what the Web was originally intended to achieve. And, although the term has become widespread in use, there is still some doubt as to whether it signifies something new or simply a case of applications catching up with the original potential (Simpson, 2009, para 1).

IBM's DeveloperWorks Newsletters interviewed Tim Berners-Lee and he stated that

> Regardless of the origins of the term and its validity, the important thing for any organization is the functionality of Web technologies. A company will not be interested in Facebook, Twitter and MySpace, etc., but in what the technology can help the company to achieve. Web 2.0 technologies include: user-generated content through wikis and Weblogs; "rich Internet applications" that employ cascading style sheets, javascript, Ajax, and Ruby on Rails, and other technologies to deliver feature-rich content to the browser; social networking; and syndication through RSS and Atom (Laningham, 2009, para 5).

Most agree the term "Web 2.0" was coined by Darcy DiNucci (author and Web expert) in 1999. In her article "Fragmented Future," she wrote:

> The Web we know now, which loads into a browser window in essentially static screenfuls, is only an embryo of the Web to come. The first glimmerings of Web 2.0 are beginning to appear, and we are just starting to see how that embryo might develop. ... The Web will be understood not as screenfuls of text and graphics but as a transport mechanism, the ether through which interactivity happens. It will appear on your computer screen, on your TV set, your car dashboard, your cell phone, hand-held game machines, and maybe even your microwave (para 10).

The term Web 2.0 does not have any standard or accepted definition by the majority of professionals or users in the Web Community. It is a hotly debated term, sometimes propagated for marketing reasons to promote the annual O'Reilley Web 2.0 Summit conferences. The O'Reilley conferences are commercial conferences started around 2005, hosted by O'Reilley Media Inc. and its CEO Tim O'Reilly, to promote discussion and training on Web 2.0 subject matter. Their desire is to put the power of the Web (e.g., technologies and collective intelligence) to work in a business environment to enhance information sharing, collaborations, and company profit. The terms Web 1.0 and Web 3.0 are equally undefined but many opinions exist. In particular, Web 1.0 only has meaning by reference to Web 2.0. As for Web 3.0, there was a brief time in 2008–2009 when it was accepted as a legitimate generational term but later its usage (as Web 3.0) was dropped and the term "Semantic Web" replaced it, with no reference to a given generation. Thus, Web x.0 generational definitions are highly subjective or speculative, not formalized, or thought not to exist at all.

Web 2.0 Web site Examples (not all inclusive): Web 2.0 Web sites are diverse in nature and provide a wealth of versatility in their specific areas of expertise or domain(s) of application. Almost any topic you can think of has a Web site dedicated to it. Many Web sites span several topics and are rich in content and participation. Many Web sites exist only to share information or to offer broad assistance to its users who desire to solve problems. The utility of the Web 2.0 Web sites is diverse, innovative and useful in many different business or military endeavors (e.g., dissemination of daily command information or interactive online workshops solving project problems or creating collaborative deliverables). In this manner, the Web sites can act as "Swiss Army Knives" and applicable to many demanding information tasks.

Web 2.0 Web site examples include: Army Knowledge Online (information mall), Amazon (seller), eBay (seller), YouTube (video sharing), Facebook (social networking), MySpace (social networking), Craigslist (selling and social interaction), Wikipedia (information sharing and problem solving), del.icio.us, Skype (telephone), Flickr (video sharing), Blip.tv, LinkedIn (professional social connections), dodgeball, and AdSense. Accessing those sites online would provide a better introduction to their diversity and versatility. Also see the Technologies section paragraph E below for associated and representative Web 2.0 technologies and applications related to the Web sites.

Web 3.0: Web 3.0 (now known as the Semantic Web) is basically forecasted to be a "Read, Write and Execute" online Web environment, a very open and intelligent online WWW collection of entities. Being "semantic" in nature (i.e., possessing "meaning"), it is supposed to better support searching, data portability and interoperability by allowing Web applications and services at various locations to transparently understand the content from other Web sites.

> The debate over Web 3.0 is hot. It is a very controversial topic.
>
> Some view it as a Data Web, the early stages or foundation for an Artificially Intelligent Web, or the realization of the Semantic Web and Service Oriented Architecture (SOA). Some view Web 3.0 as an expanded collection of various foremost harmonizing technology developments that are growing to a new level of maturity simultaneously (ubiquitous connectivity, network computing, open technologies, open identity, intelligent Web, distributed databases, and intelligent applications). (RoseIndia Web, 2007, para 3)

Web 4.0: Web 4.0 is a supposed future Web generation not yet realized or even fully visualized. Research revealed no significant Web 4.0 data content, however Internet discussions (blogs) thought there might be a generation after Web 3.0 called Web 4.0 and provided insight into an informal definition for Web 4.0 (and those generations that might follow it). Impressions were Web 4.0 would be an artificially intelligent Web with significant autonomy. An example of what one person (Willem Kossen) "thought" Web 4.0 might entail in the future is:

> Web 4.0 is the Web that extends to the real world. It's the Web of things. where your house becomes part of the Web, and your car. Where your body becomes part of the Internet. Where you DM your Thermostat using http://twitter.com to turn the heat up because you are home early. Where the refrigerator orders milk

> when it notices it's running out. Where your car checks the Google-Calendar of you and your garage to make a service appointment and where your general practitioner is notified of changes in your glucose-levels in your blood automatically and remotely. It's the Web where a seat in a plane is automatically registered when the location in your Google calendar is remote and a taxi is already waiting to pick you up, without you even thinking about it. (Kossen, 2008, para 5)

Gov 2.0 Discussion: Government 2.0 is the U.S. Government version of Web 2.0 and is its own interpretation of Web 2.0 technologies.

> The phenomenon of Web 2.0 is not about technology as much as it is about real-time communication and connection, both private and public, wherever you are. The best Web 2.0 applications have become popular because they encourage interaction among passionate participants:
>
> - Social networks encourage people to form ad hoc networks around shared interests.
> - Wikis allow answers to difficult issues to arise organically from the collaboration of enthusiastic participants.
> - Blogs communicate to a broad audience and elicit rapid feedback.
> - Portals speed communications and aggregate useful content (or mashups) from across networks.
>
> With these tools and a solid enterprise foundation, Gov 2.0 can support the information-sharing that is so crucial for openness and transparency. The opportunity is to bring Web 2.0 into the Government in a way that complements the multitude of existing systems used across agencies. An enterprise approach supports interoperability with existing and future investments, helps to enhance security, and helps you interpret citizen input. A platform for Gov 2.0 must make it easy for people and Government to communicate and collaborate in a variety of ways. The ideal platform:
>
> - Allows people to share and reuse information easily over the Web, including video and audio.
> - Provides quick and easy access to critical data and information.
> - Integrates communications, including e-mail and voice mail, along with blogs, texts, and wikis.
>
> A platform for Gov 2.0 should support social computing and the efficiencies it offers by:
>
> - Providing team workspaces, dashboards, or portals that make cross-agency collaboration and information-sharing easy.

- Defining workflows that clarify regulatory requirements or conform to a chain of approval. - Reusing information stored in existing systems that manage projects, records, accounts, and other centrally located data.
- Supporting IT diversity—interoperating with other systems; welcoming open source, commercial, and hybrid software; and using the capacity in the cloud to scale services cost-effectively. (Microsoft, 2009, p. 5-9).

Web 5.0 Definition Data: Naturally, the futuristic Web 5.0 is not defined, however, online informal discussions do provide limited information on its tentative definition. Other online sources say Web 5.0 does not exist at all. Here is one opinion:

> Web 1.0 was primarily a publishing and transactional environment. Web 2.0 as a space where users co-create value. Web 3.0 as a semantic space where machine intelligence combines with human intelligence to create new insights. Web 4.0 as a mobile space where users and real and virtual objects are integrated together to create value. Web 5.0 a sensory emotive space where we are able to move the Web from an emotionally flat environment to a space of rich interactions. (Kambil, 2008, para 2)

And, another opinion:

> Science fiction does not come close to the awesome reality of the future Web 5.0. The fictional Borg was the ultimate cyber nightmare- enclosing humans in a seductive social matrix that provided for every personal need but took away all vestiges of personal freedom. Could Web 5.0 take control and offer salvation to humanity or replicate the Borg? Web 2.0—we know well. It has delivered in a creative frenzy over the past 5 years a mixture of increasingly sophisticated social media- Web sites, blogs, feeds, wikis, multi-media, social networks and virtual worlds- followed by a cornucopia of Web services, both for personal and enterprise use—online buying and selling, booking and scheduling, location-based tracking, personal relations and communication, content discovery and selection, etc. The Semantic Web 3.0 is just starting to emerge from the kaleidoscopic mayhem of Web 2.0. It promises to automatically interpret and understand the tsunami of data generated by our cyber-culture. To achieve this, Web 3.0 searches for patterns, relationships, networks and logical inferences seamlessly integrating and exploring these more effectively and efficiently than humans. It promises some measure of redemption for the mayhem caused by its older and brasher sibling, with the potential to achieve greater processing flexibility and savings in time and effort. But already flexing its mental muscles is Web 4.0- a truly intelligent entity seeking to leverage the gains of Web 2.0 and 3.0 in more creative ways and become its own master. It promises to employ artificial intelligence techniques to analyze, optimize, control and automate most of the processes around us and do it better than humans. These are the same techniques that life has refined through evolution since it began on earth and we are now mimicking -

evolutionary algorithms, swarm intelligence, fuzzy logic, neural networks and intelligent agents. Through the medium of the intelligent Web they are already being refined and applied in the service of the myriad needs of human civilization. Within 20 years, Web 4.0 will be ubiquitous- able to interact with the repository of almost all available knowledge of human civilisation- past and present, digitally coded, semantically organised and archived for automatic retrieval and analysis. Human intelligence will have co-joined with advanced forms of artificial intelligence, creating a higher or meta-level of knowledge. This will be essential for supporting the complex decision-making and problem solving capacity, required for civilization's future progress. But this is not science fiction- this will be real. Humans have long since abdicated control of everyday living to computers and now the Web. Who bothers to check formulas for credit card payments or phone and electricity metering, let alone the more arcane algorithms that control our traffic lights, GPS systems, intensive care wards, air traffic flows, power and nuclear plants, computer and communication networks, stock market derivatives and economic models. A few specialists- but as shown by the world financial collapse, while humans may be theoretically in control, eventually the complexity, rate of change and time constraints overwhelms the quality of their decision-making and they increasingly outsource their knowledge to specialized automated software systems and Web services that can adapt faster and never get tired. But complex algorithms running on error-prone operating systems, within massive networks, especially a network of networks as fragile as the Internet, can also make horrendous mistakes as well as depersonalize human experience. And then, just as we thought we knew our future trajectory, out of the shadows emerges—Web 5.0. Web 5.0- the Wise Web, is still in shadow play, but it's definitely coming. It's signature is written large in research labs across the planet, where everything from human behavior, emotions, decision-making, network science, brain cognition and automated learning is being funded. What's emerging is a more complete understanding of human nature, consciousness and creativity and what it takes to replicate this essence in an alternate system. Web 5.0 will scoop up all this new knowledge and the intelligence offered by Webs 2.0, 3.0 and 4.0 and deliver it in an ethical, self-aware and sentient framework, embedding all biological and artificial life within a global cooperative intelligence. The Wise Web will mark the beginning of a new threshold in human civilization- a new form of global consciousness- in which all life will be embedded. All critical decisions affecting our planet and life, including those relating to global warming, sharing vital resources and the ethical resolution of conflict and human rights, will be guided by this global intelligence. (Australia.to News, 2009, para 1—10)

C. COST DATA

Obtaining sensitive cost data related to the general Web or specifically to Web 2.0 was difficult. Organizations were not willing to share their internal cost data (tough economic times), or their budgets and past financial records only allocated funds to specific hardware, software and network components without aggregating it specifically to the Web or Web 2.0. One Program Manager thought the Web costly and hard to budget (over $200K a year minimum). Thus, this research had to rely on what little information was shared or what was available publicly on the Internet.

Since significantly before the year 2000, the cost for hardware and software has steadily declined. Computers, their software, and components (memory or hard drives) have become more affordable to nearly everyone. This affordability and their ease of use has sparked numerous home or small business persons to start their own online endeavors, some for profit and some just for fun. Today, many online software Web applications are free to use (e.g., Twitter or YouTube). Some of these free Web sites, like free search engines, expose you to brief advertising as a means to gain revenue for operation of their Web site. Others "not free" sites charge a small nominal fee or subscription to access their content. Some sites require you to upload your free content in exchange for their free content (i.e., the old barter system). Along the way, the owners of Web servers, Web content and software have become more distributed, more personal and not held (managed) by large traditional computing firms (e.g., IBM). However, some small companies have indeed grown large and are very profitable today (e.g., Google). This has been true for many Web 2.0 endeavors (and technologies), in that people have aggressively shared and collaborated on their Web content, most at least initially free or at low costs. It is obvious that using free or low cost software or services saves on internal acquisition costs (purchases), but also the integration and operation of these free items into business operations have created synergy, propelling that business in the market place (competitive advantage) while increasing their exposure, sales and profit.

Web 2.0 costs must include acquisition (hardware, software and network—commercial blogging/Wiki/Social Networking platforms about $100–200K each), installation and implementation, training, maintenance, spare parts, IT employee salaries,

audit systems (performance metrics), security systems, and platform upgrades (and software patches) over time. Where possible, free products and services must be employed provided they are safe and secure (e.g., Ning at http://www.ning.com offers free Social Networks that you create "on the fly"). A life cycle view of all costs must be embraced to understand the full cost of employing Web 2.0. Additionally, one needs to understand the cost and impact of not employing Web 2.0 in its entirety (e.g., loss of competitive advantage and cost savings). Tradeoffs can serve as a business compromise on what parts of Web 2.0 to engage over time (whole or phased partial implementations).

Overall, businesses are likely to have lower overall costs from using Web 2.0 technologies based upon the synergy they provide and the benefits to the workforce. It is envisioned this cost reduction trend will continue as Web 2.0 matures and evolves into Web 3.0 and beyond. Today's younger employees are more technically savvy and more willing to share information content and work collaboratively to solve other's problems. Numerous online forums exist just for that purpose, to provide answers to business issues or problems. As time moves on, the author expects more online content and services to be freely shared, and maybe "just in time consultant" groups will come together to collaborate and maybe even get paid for what they do (or get free content exchanged instead, or future assistance for their own issues). Thus, the cost of business operations through the use of Web 2.0 technologies, and Web 2.0 products and services themselves appear to be cheaper in the future.

D. SCHEDULE DATA

Not much data existed specific to Web or Web 2.0 schedule data (e.g., times to acquire, install, configure, operate, maintain or replace). Most organizations do not intentionally keep this type data related to the Web or Web 2.0. However, it might be good as a Best Practice to record this information and use it as a performance metric. One Webmaster estimated his Web operations time durations: short term 2–4 weeks, moderate 6–12 weeks and long term over 12 weeks for setting up his environment. Thus, the research had to rely on what little information was shared or what was available publicly on the Internet.

General Web site implementation today requires less time than past implementations, especially for small personal Web sites. You can create your own Web site using commercial software that you buy or by using free downloadable software from the Internet (do it yourself), or by using online host sites that provide you free Web page templates and content that they help to establish. Some are free, paid or by subscription or by bartering (exchanges of items or services of value). The time to create a Web page with a template or the use of Web authoring tools can be as little as 10–30 minutes or less depending on the page's complexity and multimedia content. To set up a personal Web site can take 1–3 days (or less) depending on its complexity and the visuals employed. Typical organizational Web sites require approximately 1–3 weeks to establish the sites. Previously established or "Canned" Web sites can be purchased or the endeavor can be totally outsourced. To own the hardware, software and network components can be relatively expensive (small implementations $5–20K or large enterprise implementations $100–500K or more). The author experimented with many Web 2.0 technologies, tools, and Web sites, and none took more than 10 minutes to acquire and actually use. The ease of use of these items, and their free online nature facilitated these endeavors.

Web 2.0 provides a great amount of synergy, too. If you can not establish a Web site quickly by yourself, you can freely collaborate online to get it done (problem solving assistance). If you don't have the software, you can buy it online or download a free copy in less than 30 minutes or you can hire someone to perform it for you, provided you are willing to pay. The only issue with Web 2.0 schedules is its rapid growth and the related abundance of products, tools and services that are emerging daily (information overload). You need to search and monitor Web 2.0 weekly to see what is new or to discover what others are doing with its old or new technologies (new activities or business applications). Given the supposed emergence of Web 3.0, the new Web generation should provide more time savings as the Semantic Web should facilitate more efficient and faster Web searching.

E. PERFORMANCE DATA

Not much data existed specific to overall Web or Web 2.0 performance data. Some data did exist for search engine quality and information retrieval, or Web page loading speed or Web server performance. Thus, the research had to rely on what little information was shared or what was available publicly on the Internet.

Web 2.0 initiatives (technologies) have the potential to improve an organization's performance or to leverage synergy internally or externally. Innovative means will evolve as described below:

> For example, blogs will be created for all executives and department-level directors so that they can share news and announcements. All employees will have a Really Simple Syndication (RSS) reader, allowing them to subscribe to executive blogs and their department head's blog. This will enable them to receive timely updates about company business. Wikis will also be provided to all departments for information sharing and project collaboration. Finally, a company-wide social network will be created. Each employee will automatically receive a profile on the social network, **…**Employees will be able to use the network to locate employees outside their own office who they may want to collaborate with on new projects (Newman & Thomas, 2009, p. 25).

Numerous benefits evolve from Web 2.0 use (not all inclusive) include:

- E-mail Reduction
- Increased internal and external communications (employee, manager and customer)
- Decreased Information Search Time
- Increased Employee Collaboration (less stress and higher morale)
- Better Employee Recruitment and Retention (through social networking)
- Increased organizational performance (project collaboration)
- Better support for a Service Oriented Architecture
- Better support for internal organizational information discovery (data fusion, Common Operational Picture or "internal pulse" and health of an organization through technologies such as Twitter)
- Decreased cost, schedule realization, and enhanced performance

The use of the Web, or any of its current or future generations, can have both good and bad effects upon organizational work accomplishment and morale. Policy must be in place to guide Web use (governance, risk management and compliance), and all employees must exercise responsible Web use (e.g., use it only for official business while at work and not personal pleasure).

> Despite all the advancements Web 1.0 and Web 2.0 brought us, when used incorrectly, it could be harmful and wasteful. How much time is wasted every day dealing with e-mails and surfing the Web? How many employees have spent a significant amount of time during business hours downloading music and chatting with friends over Instant Messaging instead of working? Technology does not decide what's right or wrong. We have to make those decisions and then use technologies in our own best interests (Newman & Thomas, 2009, p. 10).

Constructive use of the Web and its generations (especially Web 2.0) can enhance performance. Such is the case at DISA.

> DISA has a new Forge.mil Web site that acts as an online capability to support testing Net-centric Enterprise Services (NCES), software development and other type live operations within an unclassified and secure "plug and play" environment. The new capability is similar to an online Systems Integration Lab but with expanded capabilities. Access requires a Common Access Card (CAC) and a registered account (GCN, 2009, para 2).

To properly manage and influence "performance," initial standards must be in place and managed to guide performance, along with audit controls to ensure adherence to policy. Similarly, corrective action must be taken to regain proper performance, or to modify activities to gain efficiencies during performance. A key to this is avoiding past mistakes. Here are a few mistakes to avoid as reported in Lessons Learned:

> **The Six Fatal Mistakes: What to Avoid When Implementing a Performance Management Initiative:**
>
> **Mistake Number 1: We Over Complicate the Process:** Do not over complicate the simple with our overreliance on the notion that complexity –because it is difficult to comprehend – has to be intelligent. Keep it simple. Do not over measure or over analyze.
>
> **Mistake Number 2: We Measure the Wrong Things:** The value in a performance measure is not in the measure itself but in the questions it forces you to ask about your services. Focus on measuring only Mission Critical Services. An output is an input to an outcome. Good result measures take lots of work. Keep it simple.
>
> **Mistake Number 3: We Don't Engage the Workforce:** Do not assume executives know best. Be careful of locking into a set, long term course. Never develop metrics of performance for services in the absence of a diverse, independent and decentralized group of employees and stakeholders. Performance Management is a dynamic, iterative, sometimes painful process of organizational learning and growth.

Mistake Number 4: We Perpetuate "Siloed Thinking": The process of dividing organizations into functional groups is referred to as "categorization," and is considered to be responsible for establishing the social boundaries that determine group interaction. Unfortunately though, categorization can have both positive and negative effects on an organization. Categorization is a necessary function to create specialization in organizations; it also produces far reaching and unpredictable consequences for group interaction (i.e., social dysfunction). There are many drivers behind "Siloed Thinking" (stovepipes), the most pervasive among them is competition between functional and/or structural groups over scarce resources – money, prestige, credit, employees, etc. "Siloed Thinking" (not sharing) is the single greatest impediment to organizational growth and improvement, and probably the most destructive manifestation of organizational culture run amok.

Mistake Number 5: We Declare Victory at the Wrong Time: A performance measure, like a stethoscope, is only as useful as the questions we ask of what it is telling us. A performance measure is simply a diagnostic tool. Nothing more. Nothing less. The value of a performance measure is not so much in the measure itself, as it is in the questions it forces you to ask – this is how we learn and grow as organizations.

Mistake Number 6: We Fail to Institutionalize the Performance

Initiative Throughout the Enterprise: If we are truly going to become performance informed organizations, our performance perspective has to become hardwired into the very DNA of the organization's culture. By addressing the first five Mistakes, we begin the process of socializing the initiative throughout the entire enterprise. Do not let the budget office drive your initiative. Do not fear failure. Failure is an essential ingredient in the learning process. Where we get in trouble is when we confuse performance failure with losing – which is just flat wrong. So pick up your highlighter and mark this next statement: We only lose when we fail to take action on performance failure! Failure in the pursuit of a performance target is still success if we learn and grow from the event. Failure is fundamental to performance improvement, and we have to allow the workforce to fail. If we don't, the performance effort will likely fail (Baum, 2007, p. 1-10).

F. TECHNOLOGY DATA

There is no one authoritative source that might elaborate on exactly what technologies actually constitute "Web" or each generation of the Web (DoD or commercial) or for Web 2.0 itself. Additionally, there is no agreed consensus, however there is much speculation. The Applied Project author conducted general research and surveyed online Web sites, consulted Subject Matter Experts, and inventoried the commonly used Web technologies in use at the time of data collection. The list below constitutes the majority of technologies in popular use today at Web 2.0 Web sites (not all inclusive). Web 3.0 is still new and not widely implemented (and might not exist). Also, during this possible time of transition from Web 2.0 to 3.0, technology lines between Web 2.0 and Web 3.0 may blur and overlap. Perhaps this "gray area" between generations leads people to be confused on whether a given generation exists or not, since there is no clear distinction or boundary between the various generations. And again, many say that Web "generations" do not exist at all. Here is a comparison of Web 1.0, 2.0, and 3.0 as defined in this research:

Table 1. Web 1.0 versus Web 2.0 versus Web 3.0 Comparison

WEB 1.0 VERSUS WEB 2.0 VERSUS 3.0 COMPARISON (Example Products, Capabilities, Opinions and Facts)		
Web 1.0	**Web 2.0**	**Web 3.0**
Was (older Web) Years 1992-2004 (mostly after 2001) Baby Boomers	As Is (today's Web) Year 2004 to Today Generation X	To Be (future Web) 2008 Year and Beyond Generation Y
Retronym Derived from and based upon the definition of Web 2.0	Term was first used by Dale Dougherty and Craig Cline, and shortly after, became notable after the O'Reilly Media Web 2.0 conference in 2004 The "Web 2.0" service mark registration by the company United Business Media passed final Department of Commerce United States Patent and Trademark Office Examining Attorney review on May 10, 2006,	Highly Speculative Aspects of the internet which, though potentially possible, are not technically or practically feasible at this time. Web 3.0 is a phrase coined by John Markoff of the New York Times in 2006.

WEB 1.0 VERSUS WEB 2.0 VERSUS 3.0 COMPARISON (Example Products, Capabilities, Opinions and Facts)		
Web 1.0	**Web 2.0**	**Web 3.0**
	and was registered on June 27, 2006.	
Read Retrieve Information	Builds upon Web 1.0 Read, Write Network as a Platform (run applications through the browser)	Builds upon Web 1.0 & 2.0 Read, Write, Execute Semantic Web Intelligent Web
Author to Reader Person to Content My Mind Closed Source	Person to Person(s) Collaboration & Content Social Networking Our Minds (1 to 1 or 1 to group) Synergism Open Source	Upon Demand (content or people or processing) Hypercities Global Mind (all minds) World Mind Project http://www.w2mind.org/
Mostly Static Passive Information Consumption	Mostly Dynamic Active and Mutual Information Generation & Consumption	Interactive, artificially intelligent
DoubleClick	Google AdSense	TBD
Ofoto	Flickr	TBD
Akamai	BitTorrent	TBD
mp3.com	Napster	TBD
Britannica Online	Wikipedia	TBD
personal Web sites	blogging	TBD
evite	upcoming.org and EVDB	TBD
domain name speculation	search engine optimization	TBD
page views	cost per click	TBD
screen scraping	Web services	TBD
publishing	participation	TBD
content management systems	wikis	TBD
directories (taxonomy)	tagging (“folksonomy”)	TBD
stickiness	syndication	TBD

Table data captured from Wikipedia’s Web Talk forum (blogs) at http://en.wikipedia.org/wiki/Talk:Web_2.0 during the period of the research October 2008 to November 2009, Last retrieval 1 September 2009.

The Semantic Web (emerging technology) is an evolving extension of the World Wide Web in which the semantics of information and services on the Web is defined, making it possible for the Web to understand and satisfy the requests of people and machines to use the Web content. It derives from World Wide Web Consortium director Sir Tim Berners-Lee's vision of the Web as a universal medium for data, information and knowledge exchange (Berners-Lee, Hendler & Lassila, 2008, para 1).

1. Web Site Survey Data

No authoritative source exists that counts the quantity of Web sites worldwide. Currently there are an estimated several million or more Web sites worldwide and operational at any given time (over 300 million NetCitizens in China alone), each Web site with a large number of Web pages (10–100 or more) that themselves may employ Web 2.0 technologies on the individual pages. More new Web sites are being created daily and it is impossible to survey them all. The author sought to determine an appropriate sample size to survey to achieve a 95% confidence level and a Margin of Error of 10% for the Web sites worldwide. The sample size calculator at the iSixSigma Web site could have been used, provided the population of Web sites worldwide was known (the quantity), but that population was not known (http://www.isixsigma.com/offsite.asp?A=Fr&Url=http://www.surveyguy.com/SGcalc.htm). Thus, the resultant sample size to be surveyed could not be determined. It was anticipated that, even if the quantity of Web sites worldwide was known, the sample size might be enormous and not practical to survey. Reluctantly, the author chose a limited subset of Web sites (100) at random to ascertain whether or not they used Web 2.0 at all, and if so, explore their Web 2.0 characteristics. These Web sites chosen were local military (Fort Huachuca, AZ and Army) and civilian (city government and commercial businesses), and some state and national Web sites.

One hundred Web sites were randomly surveyed to see if they used any Web 2.0 products or services. To some degree, all Web sites (100%) were using Web 2.0 technologies or accessing online products and services from other Web 2.0-enabled Web sites. It was difficult to find any online Internet entity that is not Web based or using Web 2.0 (or some portion thereof). Some probably do. A few older FTP sites still exist, but they, too, have evolved to use HTML Web-based tools to access their content. Thus, the Web is in general use everywhere online on the Internet, and Web 2.0 products and services are very prevalent (whether they call it officially Web 2.0 or not). This was true with both military and civilian Web sites. It should be noted that the Pentagon and Army do indeed use the term “Web 2.0.”

Many commercial companies are getting into the Web 2.0 business too, and providing Web 2.0 products and services. Such is the case with Microsoft as viewed from its Web site:

> Microsoft provides these Web 2.0 technologies:
> - Blogs (Sharepoint)
> - Wikis
> - Video and Multimedia Sharing
> - Photo Sharing
> - Podcasting
> - Virtual World
> - Social Networking sites
> - Syndicated Web Feeds (RSS)
> - Mashups
> - Widgets, Gadgets, and Pipes
> - Social Bookmark and News (Sharing, Tagging) sites
> - Micro-Blogging, Presence Networks
> - Gov 2.0 Data Mining and Aggregation (Microsoft, 2009, p. 16–17).
>
> The most Popular Web 2.0 Applications per Microsoft:
>
> **Social networking**
> - Windows Live: http://home.live.com
> - Facebook: http://www.facebook.com/
> - MySpace: http://www.myspace.com/
> - LinkedIn: http://www.linkedin.com/
> - GovLoop: http://www.govloop.com/

Collaborating

- Microsoft Office Live Workspace: http://workspace.officelive.com/
- Wikipedia: http://www.wikipedia.org/
- Ning: http://www.ning.com/
- Nextgov: http://www.nextgov.com/
- MSN® VIdeo: http://video.msn.com/video.aspx?mkt=en-us
- YouTube: http://www.youtube.com/
- Hulu: http://www.hulu.com/
- Flickr: http://www.flickr.com/

Blogging and micro-blogging

- WordPress: http://wordpress.org/
- Twitter: http://www.twitter.com/

Assigning meaning

- Del.i.cious: http://delicious.com/
- StumbleUpon: http://www.stumbleupon.com/
- Digg: http://digg.com/
- Reddit: http://www.reddit.com/
- Newsvine: http://www.newsvine.com/ (Microsoft, 2009, p. 19).

2. Research Author Web 2.0 Experimentation and Related Data

During the period of the research data collection, 1 October 2008 through 1 September 2009, the author experimented with several Web 2.0 technologies, mostly on Web sites that employed Web 2.0 technologies. This was conducted to identify the most popular technologies, verify their existence, learn their attributes/characteristics, their ease of use (learning curve), and discover what utility they might have, both for work and in her personal life. Table 2 lists the Web 2.0 sites in the experiment (not all inclusive) and some insight into their attributes/characteristics, etc.

Table 2. Web 2.0 Technology Experimentation

Author Web 2.0 Technology Experimentation						
Technology Web site	**Attributes / Characteristics**					
	Cost to Use	**Time to Employ**	**Performance**	**Ease of Use**	**Utility**	**Comment**
MySpace	Free	Moderate	Good	Easy	Moderate	Spam high
Twitter	Free	Low	Excellent	Easy	High	Command & Control, Great communi-cations
YouTube	Free	Low	Excellent	Easy	High	Collaboration and Training
Blip.tv	Free	Low	Good	Easy	Moderate	Hosting for Videos, podcasts
LinkedIn	Free	Low	Good	Easy	Low	Professional networking for jobs and information – Web 2.0 Group
Facebook	Free	Moderate	Excellent	Easy	High	Multifaceted
Classmates.com	$49 per year Premium (but can be	Moderate		Easy	Low	Social networking but too

Author Web 2.0 Technology Experimentation						
Technology Web site	**Attributes / Characteristics**					
	Cost to Use	**Time to Employ**	**Performance**	**Ease of Use**	**Utility**	**Comment**
	free for low level membership)					commercial-ized
Amazon.com	Free	Low	Excellent	Easy	High	Feedback and Interests Tracking
Wikipedia	Free	Low	Excellent	Easy	Very High	Collaborations, References, Forums – Best of all encyclopedias and more
Flickr.com	Free	Low	Good	Easy	Low	Video & Photo sharing and blogs, good for selling (pics)
DoDTechipedia	Restricted government use	Low	Moderate	Easy	Moderate	Technical information
AKO/DKO	Restricted government use	Moderate	Excellent	Moderate	High	Diverse useful information
Classroom 20.com	Ning network free for teachers	Low	Excellent	Easy	High	Collaborations and Problem Solving related to teaching
F150Forum.com	Free	Low	Moderate	Easy	Moderate	Collaboration and Problem Solving

G. PROCESS DATA

Not much data existed specific to Web or Web 2.0 process data. Thus, the research had to rely on what little information was shared or what was available publicly on the Internet. No official process for Web 2.0 exists. The integration and use of Web 2.0 technologies have made processes easier to define, and more effective and efficient. Synergism means the processes can be leaner, faster, cheaper, and possess higher quality. Internal collaborations within processes, or the ability to effect external collaborations on

given processes create great opportunities to better define, measure, analyze, improve and control all processes. This can favorably impact their cost, schedule and performance.

> People around the world already use Web 2.0 applications to share information, build virtual communities, and connect across geopolitical, sociological, and demographic boundaries. The next generation of government—Gov 2.0—has a unique opportunity to embrace these engaging technologies to respond to citizens with increased efficiency, transparency, and openness. However, to make Web 2.0 practical for government, you need an enterprise IT strategy that provides appropriate security, scalability, and interoperability (GCN, 2009, para 3).

The processes inside Web 2.0 itself, its various implementations, applications, and Web sites, etc., will pose a challenge to management and users alike. Given Web 2.0's dynamic nature, it may be difficult to define and baseline its processes in a traditional manner, as they may rapidly change or be threaded on a global basis. It is already known that security within the processes and inter-process will be a major challenge, since sharing and openness does not favorably support security. The security concern is now at the DoD level for a decision to limit or restrict access to Social Networking sites and possibly other Web 2.0 technologies.

H. PEOPLE DATA

Not much data existed specific to Web or Web 2.0 people data. However, there was data for people as it relates to hardware, software, and networking, but mostly in general terms. Thus, the research had to rely on what little information was shared, observed, or what was available publicly on the Internet.

The quantity of people involved in, related to, or participating in Web 2.0 products and services is huge and exists on a global basis. The quantity of people online using the Web at any time exceeds several million. Management focus will need to concentrate on both local personnel and those extended on the global Internet. Additionally, security concerns for a Trusted Insider gone bad are significant, concerns that might never be solved, but will need to be mitigated. The bright side of Web 2.0 is that the synergy among organizational work groups will have great benefit (collaboration, problem solving, and information sharing).

Many people have been involved in the evolution of the Web (and for Web 2.0 too). The World Wide Web Consortium (W3) maintains a historical list (http://www.w3.org/People.html). The father of the Web (WWW) is normally thought to be Sir Tim Berners-Lee (http://www.w3.org/People/Berners-Lee/). However, some may dispute that fact as there were earlier Web experimenters before 1991, or at least experiments into foundational technologies associated with the Web before Sir Tim Berners-Lee. But Sir Tim Berners-Lee is given the credit for the Web. It is interesting that Sir Tim Berners-Lee calls Web 2.0 "a piece of jargon" (meaning it does not exist and is only a continuation of his original concept for the Web).

Commercially, Tim O'Reilly (CEO O'Reilly Media) has used the term Web 2.0 to promote his various conferences on Web 2.0 since 2004. He has written many articles on Web 2.0 such as *What Is Web 2.0, Design patterns and business models for the next generation of software*, dated 30 September 2005 (http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html). Many associate him with coining that term, but it really was Darcy DiNucci who first used that term in her 1999 article "Fragmented Future" (http://businesspromotiontechnologies.blogspot.com/2009/06/web-20.html).

Who are the Web 2.0 leaders today? Everyone on the Internet. We are in a newly emerging global collaboration and all are empowered to create and share their new Web 2.0 endeavors.

I. QUALITY DATA

Not much data existed specific to Web or Web 2.0 quality data. Quality programs were in existence, but possessed broad coverage (not just for the Web or Web 2.0). Thus, research had to rely on what little information was shared or what was available publicly on the Internet.

No specific quality information controls or metrics directly referenced Web 2.0; however, the use of quality in any endeavor is a Best Practice. The most prevalent quality program being embraced today is Six Sigma or Lean Six Sigma (http://www.isixsigma.com/). As for Information Technology (IT) Service Management

(and Web too), the Information Technology Infrastructure Library (ITIL) is a rich source of Best Practices information (http://www.itil-officialsite.com/home/home.asp). Many other "valuable" formal quality programs exist that might be used for the Web and Web 2.0 (e.g., Total Quality Management (http://www.isixsigma.com/me/tqm/), ISO 9000 series (http://www.iso.org/iso/pressrelease.htm?refid=Ref1236), and Baldridge (http://www.baldrige.nist.gov/). Basically, all quality programs provide general topic areas that should be identified, reviewed, evaluated, managed, and ideas on how to improve them (performance metrics, Lessons Learned or Best Practices). Plus many national organizations exist to standardize IT or Web operations through publication of standards (e.g., National Institute of Standards and Technology (NIST), American National Standards Institute (ANSI), and International Institute of Electrical and Electronics Engineers, Inc. (IEEE), etc.). The DoD published the DoD Architectural Framework (DoDAF) versions 1.5 and 2.0 to standardize architectures and methodologies for the military (see AKO Web site).

There are several endeavors, military and civilian, to address quality on the Web. These efforts usually revolve around securing the Web better, or infusing newly emerging technologies to make it more effective and efficient. For DoD, the Defense Information Systems Agency Information Assurance Support Environment (http://iase.disa.mil/index2.html) publishes Web security guidance in the Security Technical Implementation Guides (STIG) as assisted by commercial vendors and the National Security Agency. In the commercial arena, SANS (SysAdmin, Audit, Network, Security) Institute (http://www.sans.org/) hosts training related to Web security and provides Lessons Learned and Best Practices. So many attempt to address quality in Web environments because it makes sense to do so, because the Web is integral to their business success.

Likewise, the various national standards bodies provide regulations and standards (NIST, ANSI and IEEE). And of course, the Worldwide Web Consortia (Sir Tim Berners-Lee Chief Executive Officer) provides Web guidance on an international basis, along with the International Standards Organization.

J. SECURITY DATA

Not much data existed specific to Web 2.0 security data. Much study has been done on the Web in general, especially for securing Web components or recording attacks against Web components (mostly software attacks). Thus, research had to rely on what little information was shared or what was available publicly on the Internet.

Security is a major challenge for Web 2.0. The Marine Corps restricted its members to limited access to Social Networking Web sites effective 3 August 2009. DoD (including Army) is currently reviewing their policy on access to Social Networking Web sites and may also implement a similar limited ban. A decision is expected in the 2010 time frame. The Marine restriction:

> The Marine ban and DoD review are happening even though social media has become a significant force since the 2007 reversal of an initial DoD ban on social-networking sites. Government and the military have become deeply entrenched in social-media tools. Various military and government outfits have hundreds of thousands of Twitter followers and Facebook fans, and access to social-media sites is required on U.S. Army bases**.** However, according to the Marine order, "These Internet sites in general are a proven haven for malicious actors and content and are particularly high-risk due to information exposure, user-generated content and targeting by adversaries." The order added that social-networking sites create an easy conduit for information leaks. However, some assert that a blanket ban on social media isn't the way to go. "There certainly are security concerns associated with social networking, but it would be a step back to ban social networks completely," said information technology security expert Rohyt Belani, a consultant and instructor at Carnegie-Mellon University. "I think there is a middle ground that can be reached." That middle ground will require the incorporation of significant security measures. DoD does need a standard, department wide policy (FCW, 2009, para 3-5).
>
> Although many Defense Department officials believe social networking tools are useful, those emerging technologies will likely need to be deployed solely on the military domain and cut off from the public Internet, Robert Carey, the Navy's chief information officer, said yesterday. "There is a powerful opportunity inside the dot-mil domain for these tools," Carey said in a speech hosted by the market research firm Input. DoD officials need to figure out where it is appropriate for information on the Nonsecure Internet Protocol Router Network (NIPRNet) to be shared with social networking tools on the public Internet, Carey said. For example, military public affairs and recruiting staff members need to use social networking on the public Internet, he said. "But as far as the work-based environment, is it better to have all that stuff inside the family?" Carey asked. Meanwhile, numerous media reports that the Marine Corps banned social

> networking (totally) on all of its official computers and networks is not accurate, Carey said. Rather, that service's policy mirrors the limited use of the Web tools Carey described. The Marine Corps "allows social networking for the folks they've designated need it," Carey said. "So public affairs and recruiters have access." Carey traveled to Stanford University last week where he met with social networking technology providers that included LinkedIn and MySpace. He had to explain to the company officials that even though some Navy information is not classified; it still should not be broadcast over the Internet. Whether, and how, the social networking companies will provide their technology for the DoD's private use hasn't been decided, Carey said. "We expect to meet in September and try and move on with that," he said. "So stay tuned." (Beizer, 2009, para 1–7)

The Army is also reviewing its Web 2.0 social networking site policy. See Army interim policy guidance message (below) published 17 August 2009 by the Army Materiel Command to its subordinates:

> Alaract 228/2009—Public announcement on the army's guidance on accessing social networking sites (SNS)
>
> This message has been sent by the pentagon telecommunications center on behalf of DA washington DC//g-3/5/7//
>
> Subject: Public announcement on the army's guidance on accessing social networking sites (SNS)//
>
> Ref/a//Army Regulation (AR) 25-2, information asurance/23 Mar 09//
>
> Ref/b/Usstratcom warnord, actions to address risk of using niprnet connectivity to access internet social networking sites (SNS)/10 Jul 09//
>
> 1. (U) Current army guidance permits mission use access to internet social networking sites (SNS), unless specifically prohibited by joint task force global network operations (JTF-GNO). SNS provides an excellent opportunity to collaborate and share information; however, use of the sites could expose army networks to malicious software and create cyber-security problems.
>
> 2. (U) The army is currently reviewing its policies on SNS. While waiting for this review to be completed, there is no department of the army directive that prohibits users from accessing social networking sites. Commanders are responsible for enforcing standards of discipline within their command and all personnel must remain vigilant to ensure prudent use of information resources.
>
> 3. (U) Commanders must identify command critical information and ensure personnel receive proper OPSEC training to prevent public release of sensitive information. Current army information assurance policies, procedures and Best

> Practices are located at: https://informationassurance.us.army.mil. Until further guidance is issued, no additional tools or software should be developed for SNS. Additionally, the department of defense is developing a web 2.0 policy from a comprehensive risk management perspective no later than 30 Sep 09. (U) (AMC Electronic Message, 10 July 2009)

Web 2.0 Threat Data:

Not much data existed specific to Web 2.0 threat data, but a significant amount existed for the general Web. Traditionally, the most significant threat has been the "Trusted Insider gone bad," because they have immediate access and localized knowledge on the organization and its systems. Close to this threat are many others (e.g., Web site attacks using vulnerable browsers, Botnets, and phishing).

> The insider threat to critical infrastructure is one or more individuals with the access and/or inside knowledge of a company, organization, or enterprise that would allow them to exploit the vulnerabilities of that entity's security, systems, services, products, or facilities with the intent to cause harm (The National Infrastructure Advisory Council, 2007, p. 11).

> Insider threats exist for all organizations. Essentially, this threat lies in the potential that a trusted employee may betray their obligations and allegiances to their employer and conduct sabotage or espionage against them. Insider betrayals include a broad range of actions, from secretive acts of theft or subtle forms of sabotage to more aggressive and overt forms of vengeance, sabotage, and even workplace violence. The threat posed by insiders is one most owner-operators neither understand nor appreciate, and it is a term that is commonly used to refer to IT network use violations. This often leads to further confusion about the nature and seriousness of the threat. This misunderstanding or underestimation relates, in part, to the stigma that an act of insider betrayal carries with it – a stigma that can cause customers, partners, and shareholders to lose trust in an organization. This loss of trust can translate into lost business, revenue, and value (The National Infrastructure Advisory Council, 2007, p. 4).

> The National Infrastructure Advisory Council (NIAC) determined insider threats to be significant given their potential to cause serious consequences that cascade beyond the attacked infrastructure. The NIAC also found economic espionage poses a significant threat to the competitive viability of many critical infrastructures in the United States. Additionally, the NIAC found that awareness and mitigation of the threat varies greatly among the critical infrastructure sectors (The National Infrastructure Advisory Council, 2007, p. 5).

NIAC Recommendations to counter the Trusted Insider threat:

- Education, awareness and training (The National Infrastructure Advisory Council, 2007, Appendix E Framework)
- Employee screening
- Publish a technology policy and use Best Practices (The National Infrastructure Advisory Council, 2007, Appendix F Framework)
- Improve Information Sharing (central clearing house for threats) and use of threat statistics
- Continue to study the Insider Threat (causes, impacts and solutions)
- Research is required to develop mitigations, policy, and goals in the areas of global workforces, criminal history risk assessment, and technology challenges (The National Infrastructure Advisory Council, 2007, p. 5-8)
- The Insider Threat Best Practices framework provides an overview of the techniques and methods uncovered by the NIAC, presented in a risk controls framework approach. (The National Infrastructure Advisory Council, 2007, Appendix F)

Trusted insider attacks are not the only Web menaces. Many threats exist. The SANS Institute (http://www.sans.org) compiles a list each year of those most dangerous, the Top Ten. Many threats repeat each year and new ones emerge. For 2008, the threats for Webs were (in order of priority):

- Increasingly Sophisticated Web site Attacks That Exploit Browser Vulnerabilities - Especially On Trusted Web sites
- Increasing Sophistication And Effectiveness In Botnets
- Cyber Espionage Efforts By Well Resourced Organizations Looking To Extract Large Amounts Of Data - Particularly Using Targeted Phishing
- Mobile Phone Threats, Especially Against iPhones And Android-Based Phones; Plus VOIP
- Insider Attacks
- Advanced Identity Theft from Persistent Bots
- Increasingly Malicious Spyware
- Web Application Security Exploits
- Increasingly Sophisticated Social Engineering Including Blending Phishing with VOIP and Event Phishing
- Supply Chain Attacks Infecting Consumer Devices (USB Thumb Drives, GPS Systems, Photo Frames, etc.) Distributed by Trusted Organizations (SANS, 2008, para 1–10).

Malicious people are innovative when it comes to new technology, especially that on the Web. New tech means new ways for criminals to attack systems. Next year will see hackers get smart about cloud computing, social networking and more. Here are top ten threats to keep an eye on:

- Malware 2.0 (tailored to Web 2.0 technologies)
- An explosion in new malware variants and Web threats
- Social networking spam
- More legitimate Web site hacking (hack real site to use as a fake front for phishing)
- Unemployment creates more cybercriminals
- Security budgets unlikely to grow
- Mobile computing hacks
- The new generation of botnets (emerge)
- Cyber hacking on virtual worlds (social reality-based worlds)
- Reputation hijacking flourishes (fake sites that look real and phish) (Wattanajantra, 2008, para 1-10)

In addition to hackers attacking Web sites for fun or revenge, they also attack Web sites for economic reasons or as an act of espionage or terror.

> A recent report by security firm Finjan claimed that cybercrime is as lucrative a business as drug trafficking. Its Cybercrime Intelligence Report found that a single hacker could make as much as $10,800 (£7,300) a day, which the company extrapolated to $3.9m (£2.6m) a year. "This type of cybercrime activity is here to stay and will grow because there is so much money involved and it's hard to get caught" (Shiels, 2009, para 18).

Today, the economy is not good and organizations have a significant challenge:

> In today's tough economic environment, IT professionals are asked to do more with less. While Web 2.0 threats and browser exploits are growing, you have little or no Capital expenditure to acquire and deploy new security appliances and very tight Operating expenditure to manage them. IT management is expected to:
>
> - Protect their enterprises from botnets, malicious active content, cross site scripting and more.
> - Control their bandwidth cost that is doubling due to Web 2.0 streaming content such as YouTube (blocked on Army network).
> - Limit liability created by innocent users' blogging on Facebook, or sending Webmail with sensitive attachments (Zscaler, 2009, para 1).

The year 2008 was not a good year for Web sites and the future is expected to be no better. Web attacks and their sophistication are increasing as described below:

> In the ScanSafe 2007 Annual Global Threat Report, we predicted that Web surfers might be in for a wild ride in 2008. Unfortunately, we were correct. The year launched with wide-scale attacks on mom-and-pop style Web sites. These

> attacks persisted throughout 2008, but their volume was quickly overtaken by surges in SQL injection attacks, which were carried out via automated attack tools delivered via botnets. The success of the SGL injection attacks has been such that in July the rate of Web-delivered malware was higher than the entirety of 2007. And the rate in October 2008 was 21% greater than July." The report explains that the study "is an analysis of more than 200 billion Web requests processed in 2008 by the ScanSafe Threat Center on behalf of the company's corporate clients in over 80 countries across five continents (Kabay, 2009, para 1–2).

Compounding the problem are Trusted Insiders gone bad:

> Companies around Hong Kong and China are facing security pressures coming from their own employees trying to bypass company security policies for new Web applications, a survey commissioned by IT solutions providers Websense said. According to the Websense survey, about 54 percent of IT managers in Hong Kong and 53 percent in China admit that their users try to bypass security policies to access Web 2.0 applications (ComputerWorld, 2009, para 1–3).

A lot of software used on the Web does not possess good security:

> Nearly 80% of all hacking attacks are the result of security holes in Web applications, according to the Verizon Business report. Network managers know that their biggest vulnerability is in Web applications, so they put all of their effort into testing their critical and Internet-facing systems. The problem is that most hacking attacks leverage security mistakes in noncritical systems inside networks. "The main problem is that we're testing like crazy the critical Web applications, and we're not testing the non-Web applications," Tippett says. He recommends that network managers test all of their applications for basic vulnerabilities (Marsan, 2009, para 1–3)

K. LEGAL DATA

Not much data existed specific to Web or Web 2.0 legal data. This whole legal area is a gray area (undefined) for the whole Internet (e.g., where jurisdictions begin and end, and the protection of privacy, intellectual or proprietary rights). Thus, research had to rely on what little information was shared or what was available publicly on the Internet. Key legal challenges facing Web 2.0 use privacy protection, copyright or intellectual property infringement, identity theft, personal harassment, and the prosecution of trusted insiders gone bad and hackers (domestic and international).

The term Web 2.0 is now also a registered trademark. The "WEB 2.0" service mark registration by the company United Business Media passed final Department of

Commerce United States Patent and Trademark Office examining attorney review on May 10, 2006, and was registered on June 27, 2006 (TARR, 2006).

L. MISCELLANEOUS DATA

1. Hard-Bound Book Data

Many books are being written today on the Web, as well as on Web 2.0. The Amazon online company (www.Amazon.com) had 588,030 books on the Web, 774,150 books on the WWW, 5,118 books on Web 2.0, and 2,154 books on Web 3.0 as of 23 August 2009. Amazon itself employs Web 2.0 technologies to support its daily business operations (e.g., user feedback and review blogs). On the Internet and expressed in books, is a vast collection of data on the general Web, WWW or Web 2.0 (or Web 3.0), mostly speculation and little consensus. Information indicates people are indeed discussing and embracing the Web and its various generations, even if controversial.

> In many ways, publishing as we have known it for centuries, made the world's leading enterprises what they are today. If, as some say, knowledge is power, then managing the publishing of content has been the key to power for many enterprises. From papyrus scrolls to the printed edicts of kings and queens to typed memoranda to photocopying to e-mails to electronic databases and Web sites, publishing has driven the ability of large organizations to assemble information [intelligent content] that helps them to make effective decisions and that enables them to acquire and retain power, leadership and influence (Blossom, 2009, p. 131).

Newman and Thomas (2009) stated in their book "One of the defining characteristics of Web 2.0 is collaboration. Harnessing a multitude of people to accomplish something is good, fast and inexpensive. Synergy is achieved when groups work freely" (p. 11).

2. Interview Data

Approximately 50 people (names not recorded for confidentiality and to prevent retribution as a "whistle blower") were orally interviewed during a ten month period (military and civilian). This is a small Sample Size of the people involved with the Web worldwide and may be statistically insignificant, but still valuable. Twenty percent of the people interviewed generally knew the term "Web 2.0" but could not adequately discuss

its definition, other than to state it was probably a generation of the Web. Technical personnel (Web managers and system administrators) were most knowledgeable, but again, mostly within their specific Web implementation domains (Windows or UNIX). Most people interviewed (90%) knew the terms Web, WWW, or Worldwide Web better, and associated it with the current Internet and the Web activities occurring online via their networked computers (e.g., Sharepoint, e-mail, search engines and general Web surfing). Within the group that actually knew about Web 2.0 (the 20%), most only knew a limited subset of Web 2.0 technologies, i.e., the most popular technologies that might be associated with it (e.g., discussion boards, blogs, podcasts, Facebook, Twitter, MySpace, YouTube, and Flickr, etc.).

All interviewed saw the operational need to use Web technologies and social collaborations, and wanted to expand and leverage their Web capabilities (whatever generation) to support their business or mission requirements. Many commented their Web implementations were technically complex, costly (over $200K a year as a minimum), difficult to test, required training, not under configuration management, and had security issues (mostly permissions). The significant concern among all was securing their sensitive information, identity theft, and preventing security violations, denial of service, or hackers. Commercial companies were concerned over maintaining their competitive advantage in the market place and loss of proprietary information. DoD concerns were centered on maintaining their Joint Vision goals of Information Superiority, Full Spectrum Dominance, and Full Dimensional Protection as they pertain to ongoing or future military operation success (e.g., the wars in Iraq and Afghanistan). Web activities are deemed critical today in DoD daily operations. Many Services, including the Army, have their own controlled Web portals (e.g., Army Knowledge Online), which use Web 2.0 technologies to some degree.

Given the downward cost trends of computers, networking and the Web in general, most interviewed had adequate budgets to support their ongoing Web operations but could use more funding. Many of the new Web technologies actually saved funds (e.g., online teleconferencing to save on travel funds), or enhanced quick operational communications (e.g., Twitter). All interviewed envisioned a continuation of the Web, be

it whatever generation. Recent Marine Corps policy to deny access to social media (social networking) sites for its Marines (3 August 2009) and the pending DoD policy that might restrict or limit Web access DoD Enterprise-wide may have severe impacts on the military's use of Web 2.0 (or the Web in general). This DoD decision must be monitored and its impact assessed.

3. Newspaper Data

Article 1 (2009) *Fort Huachuca gets connected* by Scout report indicated Fort Huachuca debuted its Facebook page at the Community Commo Check on July 7. Fort Huachuca also has a Twitter account. Fort users can access news or get listings of postings as soon as they occur. Article 2 (2009) *TRADOC connects via social media* by John Harlow "Web-based collaboration tools, generally known as social media, are changing the way people stay connected. U.S. Army Training and Doctrine Command is working to leverage social media in training Army leaders to be more adaptive and agile in their conduct of operations, and to broaden discussion across the Army and with the public. Millions of Americans are comfortable in Facebook and Flickr" (p. 3).

4. Magazine Data

The DoD definitely sees benefit in the Web and Web 2.0 technologies (wikis). As new technologies emerge, DoD incorporates their use. Upon its first day operational, DTIC's Techipedia (www.Techipedia.mil) had over 1500 connected users, all using their Common Access Cards, to share knowledge "DoDTechipedia is a wiki, designed by the Department of Defense (DoD), that facilitates increased communication and collaboration among DoD scientists, engineers, program managers, acquisition professionals, and operational warfighters" (IA Newsletter, 2009, p. 4).

Web 2.0 is becoming a mainstay in many areas of life, be it military or civilian. New technologies facilitate collaboration.

> Most of us are familiar with popular Web 2.0 tools such as blogs, podcasts, and social networking sites (Facebook, Twitter, and Myspace). But there are other arrows in the Web 2.0 quiver that don't have the same familiarity or name recognition. Here's a rundown of those lesser known tools:

- *Wikis* (collection of Web pages that anyone might access to change its content to facilitate collaborative endeavors)
- [Really Simple Syndication" or "Rich Site Summary] *RSS Web Feeds* (Web feeds used to syndicate /publish online content automatically)
- *Web Services* (Cloud Computing – using software on or over the Internet without directly downloading it to your computer's hard drive)
- *Folksonomies* (User chosen keywords to organize and index onlive content to facilitate its use, especially helpful in searching)
- *Video Sharing Sites* (Allow video uploads for private or public informational sharing, or for commercial marketing purposes) (Zielinski, 2009, p.10).

> In some ways, Facebook is like a real-world get together – friends passing photos around, laughing at one another's jokes. But it's also like getting everyone you ever knew into one room for a 24-hour-a-day cocktail party with no host and few boundaries (Reader's Digest, 2009, p. 96).

5. Web Search Engine Data

Many search engines exist on the Internet (http://www.20search.com/ and http://thesearchenginelist.com/). Three search engines were arbitrarily chosen to explore the Internet for the existence and prevalence of Web information: Google, Bing, and Yahoo. The quantity of "Hits" returned on each Web topic basically showed the existence of that topic or not, and some limited idea on its popularity for discussion. Additionally, exploring each link deeper provided an idea on whether the Web site information at that specific location, or the people involved in that topic's discussion felt the topic genuine or not, and whether it had potential for operational use. Many links discussed the technologies they felt constituted that Web "generation" topic.

The sheer number of Web pages associated with each Hit was too large to explore in great detail. Hits were voluminous and contained an abundance of information related to the Web, Web 2.0, and the other generations.

Many online discussions addressed generations past Web 5.0 and beyond; however, they were deemed too speculative to include. Their data were based upon opinion and had no factual evidence to back their assertions.

Table 3. Web Search Engine Hits as of 18 August 2009

	WEB SEARCH ENGINE HITS AS OF 18 AUGUST 2009 AT 0909 AM (Quantity of Online References to the Given Topic)					
Search Engine Title	**Web / WWW / World Wide Web**	**Web 1.0**	**Web 2.0**	**Web 3.0**	**Web 4.0**	**Web 5.0**
Google	2,930,000,000 / 2,410,000,000 / 23,000,000	1,340,000	81,600,000	1,520,000	133,000	2,840,000
Bing	2,560,000,000 / 13,100,000,000 / 304,000,000	2,900,000,000	2,570,000,000	2,540,000,000	2,910,000,000	2,530,000,000
Yahoo	14,300,000,000 / 31,600,000,000 / 444,000,000	3,580,000	294,000,000	294,000,000	645,000	323,000

Hits also occurred on the topics Web 6.0 up to Web 20.0 and even beyond, but were not recorded as data. They were deemed irrelevant for this research, since they were either too speculative in nature (to some degree imaginary), too far in the future to have impact on today's Program Managers within the next 10 years, or highly subject to people and technological changes in the next 5–10 years (limited utility today).

a. Online Internet Data

New innovative uses of the Web (or Web 2.0) occur daily. One such example is the online information sharing Web site called WikiAnswers.

> WikiAnswers harnesses people's collective knowledge to give you useful answers about anything. WikiAnswers is a wiki-based Question and Answer (Q&A) project powered by contributors from all walks of life. Anyone can ask, answer or edit questions, building a global Q&A database, covering all topics. WikiAnswers, previously known as FAQ Farm, was acquired by Answers

> Corporation in November 2006 and is now part of the Answers.com family. It was founded in 2002 by Chris Whitten, a pioneer in the Q&A arena. (Answers.com, 2009, para 1-5)

Another Web example is expressed in the book Wikinomics. Tapscott, D and Williams, A (2006) in their book *How Mass Collaboration Changes Everything*, addressed successful stories on using wikis and open-source technology for mass collaboration in the early twenty first century. The authors also explained Wikinomics four basic ideas, openness, peer sharing, and action globally (Tapscott & William, 2006).

The third and best example of Web 2.0 in operation is Wikipedia (**http://en.wikipedia.org/wiki/Main_Page**). It has surpassed traditional encyclopedias in popularity and is a wealth of collaborative knowledge.

> Anyone who has done even a modest amount of browsing on the Internet has probably run across Wikipedia, the user-edited online encyclopedia that now dwarfs the online version of Encyclopedia Britannica. This is the prime example of what is called the new Web, or Web 2.0, where sites such as MySpace, YouTube, Flickr, and even the Human Genome Project allow mass collaboration from participants in the online community. These open systems can produce faster and more powerful results than the traditional closed proprietary systems that have been the norm for private industry and educational institutions. Detractors claim that authentic voices are being overrun by "an anonymous tide of mass mediocrity," and private industry laments that competition from the free goods and services created by the masses compete with proprietary marketplace offerings. The most obvious example of this is Linux, the open-source operating system that has killed Microsoft in the server environment. But is this a bad thing? Tapscott thinks not; and as a proponent of peering, sharing, and open-source thinking, he has presented a clear and exciting preview of how peer innovation will change everything. David Siegfried Copyright © American Library Association (Siegfried, 2009, para 1).

b. Internet News Feed Data (Subscription Newsletters)

Government Computer News (GCN) Newsletters. GCN is free news delivered monthly in hard copy magazine format or via electronic newsletters, or in electronic Digest format. It provides general information of interest to Federal Government employees. Subscription is provided free at URL http://www.gcn.com/Home.aspx (last retrieval 1 September 2009). During the research

period 1 October 2008 through 30 November 2009, approximately 11 monthly newsletters and 275 daily updates were received and reviewed. 100% of them had at least one reference to the Web or Web 2.0, or a related item. Web 2.0 news examples: GAO expands presence with YouTube and Twitter (GCN Issue 8 July 2009). DoD warns against the dark side of social networking (GCN Issue 19 July 2009). Twitter tools on the rise (GCN Daily Digest Issue 17 April 2009). Additionally, the GCN Web site itself uses Web 2.0 technologies (e.g., blogs, videos, and Webcasts).

And GCN writers also explored the benefits and risks of using Web 2.0 (social media) through discussions with Information Technology experts. Here is what they discovered:

> Debate continues to rage at the Defense Department over the use of social-media tools. We asked some experts to present the arguments on both sides of the debate. Here are the pros:
>
> - Web 2.0 technology improves collaboration.
> - It streamlines internal and external communications.
> - It costs little or nothing to use.
> - It has the potential to attract to young recruits to DoD.
> - It's highly portable.
>
> … and 5 reasons why it [DoD] shouldn't [use Web 2.0]:
>
> - Sensitive information is on the public Internet.
> - The tools can make it difficult to comply with federal regulations.
> - The technology lacks standards.
> - Sharing personal information can put employees at risk.
> - The tools demand a lot of bandwidth.
>
> Web 2.0 is more of a philosophy than architecture. (Beizer & Corrin, 2009, para 1–10).

Information Assurance Technology Analysis Center (IATAC) Newsletters. The IATAC is a weekly (e-mail) or daily (Web site only) news service for official Government use and is delivered electronically (Digest format). It provides general information on evolving technologies of interest to the Federal Government and its contractor employees (emphasis cyber security). Subscription is provided free to authorize personnel at URL **http://iac.dtic.mil/iatac/IA_newsletter.jsp** (last retrieval 1 September 2009). During the research study period 1 October 2008 through 30

November 2009, approximately 86 newsletters were received and reviewed. One hundred percent of them had at least one reference to the Web or Web 2.0, or a related item. The IATAC Web site had information daily on the topics. Web 2.0 news examples: *U.S. Army warns of Twitter attacks* (IATAC Digest 27 October 2008). *Navy encourages use of Web 2.0 tools* (IATAC Digest 30 October 2008). *A year after YouTube ban, Pentagon launches TroopTube* (IATAC Digest 13 November 2008). *On 1 Oct 2008, the Defense Technical Information Center (DTIC) with the Director of Defense (DoD) Research and Engineering announced the launch of DoD Techipedia, a DoD scientific and technical wiki* (IATAC Digest 8 December 2009). *Google on the prowl, Web attacks increase, Social Networks unravel.* (IATAC Digest 5 January 2009). *Unauthorized Web use on the rise* (IATAC Digest 5 February 2009). *Vendors call for Cloud Computing standards* (IATAC Digest 30 March 2009). *Milkeyy Attack Hits Twitter Users – a Bad 25 Hours for Web 2.0 Security* (IATAC Digest 13 April 2009). *The 5 Essentials for Safe Online Socializing* (IATAC Digest 4 May 2009). *Sun Launches Cloud Services Portfolio* (IATAC Digest 1 June 2009). Additionally, the IATAC Web site itself uses Web 2.0 technologies (e.g., Ask an Expert for collaborations).

SANS (SysAdmin, Audit, Network, Security) Institute Newbites. SANS is a free weekly newsletter delivered via e-mail. It provides information of interest to the public (emphasis on cyber security and vulnerabilities in technologies). Subscription is provided free at URL **http://www.sans.org/** . Last retrieval 1 September 2009. During the JAP generation period 1 October 2008 through 30 November 2009, approximately 58 newsletters were reviewed. One hundred percent of them had at least one reference to the Web or Web 2.0, or a related item. Web 2.0 news example: *Former Employee Admits Deleting Information From Government Computer System* (SANS Newbites 27 January 2009). *Phishers Lure Users with Offer of Economic Stimulus Payments* (SANS Newbites 10 February 2009). *Wikileaks e-mails Sen. Coleman Campaign Donors About Data Leak* (SANS Newbites 13 March 2009). Additionally, the SANS Web site itself uses Web 2.0 technologies (e.g., blogs, RSS feeds, audiocasts, and Webcasts).

Federal Computer Week (FCW) Newsletters. FCW is a free weekly newsletter delivered via e-mail. It provides information of interest to Federal Government employees (e.g., Gov 2.0). Subscription is provided free at URL **http://www.fcw.com/Home.aspx** (last retrieval 1 September 2009). During the research generation period 1 October 2008 through 30 November 2009, approximately 44 newsletters were received and reviewed. One hundred percent of them had at least one reference to the Web or Web 2.0, or a related item. Web 2.0 news example: "As Federal agencies evolve and mature IT operations and infrastructure, the concepts of Cloud Computing and "software as a service" have emerged as critical approaches to meeting unique mission requirements" (FCW, 29 April 2009). Additionally, the FCW Web site itself uses Web 2.0 technologies (e.g., blogs and Webcasts).

National Security Institute's (NSI) Security NewsWatch Newsletters. NSI Security NewsWatch is a free roundup of news, trends and issues of concern for busy professionals. It is a complimentary news service distributed twice each month via e-mail. NSI's Security NewsWatch provides briefs on security trends, technologies, Best Practices, legislation and critical issues. Subscription is provided free at URL **http://nsi.org/newswatch.html** (Last retrieval 1 September 2009). During the research study generation period 1 October 2008 through 30 November 2009, approximately 22 newsletters were received and reviewed. One hundred percent of them had at least one reference to the Web or Web 2.0 (security or non-security), or to infrastructures that support them (included threats manifested in that two week period). Web 2.0 news example: *NSA joined social network for intelligence analysts* (NSI Security NewsWatch Issue 13 March 2009).

Army Knowledge Online / Defense Knowledge Online (AKO/DKO) Advisor Newsletter. The AKO/DKO Advisor is an official monthly newsletter for authorized users on the AKO/DKO. During the research generation period 1 October 2008 through 30 November 2009, approximately 10 newsletters were reviewed. One hundred percent of them had at least one reference to the Web or Web 2.0, or a related item. Web 2.0 news examples:

AKO/DKO is continually working on adding to and improving its Web 2.0 capabilities—and November was no exception. The latest portal upgrades brought a number of improvements to the My Profile page, many of which were suggested by users. For example, it is now possible to add a photo to your profile. Don't be shy! This feature is beneficial for those who remember your face but not your last name, or for those who need help differentiating between individuals with common names. **Why the Focus on Web 2.0?** Unclear on why various types of interactive features are being added to the portal? All DoD organizations are unique not only in their job duties, but also in their mobility. Not only can the new My Profile features help friends reconnect, but they make quick work of identifying individuals who have a specific professional expertise. (AKO/DKO, 2008, p. 1–3).

IV. ANALYSIS

A. DATA ANALYSIS OVERVIEW

The research author performed analyses on all the data collected, discussed, and encountered during the research period, including individual datum and data in aggregate. Before discussing the specific Web 2.0 data collected and its various analyses, the issue of whether Web 2.0 actually exists must be first addressed. If Web 2.0 does not exist, then there is no tangible, specific "Web 2.0 data" to analyze, except the various general statements that Web 2.0 does or does not exist. However, there is an overwhelming abundance of global data and expert opinion that Web 2.0 does indeed exist in some form, even if it is not formally recognized, defined, configuration managed, or documented by any authoritative source, United States or other. It is unfortunate that Web 2.0 has not been legitimately characterized into some type of technical and non-technical baseline that clearly delineates its abilities, capabilities, technologies, boundaries, and operations. Likewise, there are no clearly defined Web 2.0 technical, systems, or operational architectural views to evaluate for Web 2.0 compliancy.

The general proof that Web 2.0 most likely does indeed exist:

- Web Search Engine hits in excess of 81 million up to 2 trillion people worldwide occurred on the topic "Web 2.0." A large quantity of people believe in and are discussing, implementing, enhancing, and writing about Web 2.0 as a legitimate topic.
- Amazon.com books on the topic "Web 2.0" exceeded 5,118 in quantity as of 23 August 2009. People consider it to be a real and legitimate topic on which to write. Many books describe how to implement Web 2.0 while other books discuss current implementations in place today.
- Governmental organizations use the term "Web 2.0" as a real, legitimate entity in their routine discussions, plans and reports, architectures, and on their Web sites (e.g., Army Knowledge Online, Information Assurance

Technical Analysis Center, Army Materiel Command, Marine Corps policy statements, and DoD pending Web 2.0 policy guidance).

- The quantity of Web sites using what they term "Web 2.0 products and services" is hundreds of thousands. The author personally experimented with over 14 specific Web 2.0-type Web sites and found they did exist, and they conform to the general notion of what a Web 2.0 implementation should possess: read and write capabilities with social media input.
- Numerous commercial conferences exist on the topic of "Web 2.0" (e.g., O'Reilly and Associates Web 2.0 Summits, past and present). Many conferences have occurred since 2006 and the next Web 2.0 Summit is scheduled 20–22 October 2009. The people organizing these conferences, the people paying money to attend, and the actual attendees view Web 2.0 conferences as beneficial, hence their recurring attendance since 2006. This is a large group of people worldwide that view Web 2.0 as a legitimate entity that does exist, and they want to use or enhance it.
- Numerous commercial newsletters, magazines and newspapers routinely address the topic of "Web 2.0" within their literature as a bona fide subject (e.g., Government Computer News, Fort Huachuca Scout, and Federal Computer Weekly). Many articles address current Web 2.0 implementations, their utilization or pros and cons of operations.
- The U.S. Patent and Trademark Office officially registered the term "WEB 2.0" on 27 June 2006 to United Business Media. They both consider Web 2.0 legitimate and sufficiently relevant to formally trademark. To gain a trademark, "something" must exist in sufficient form to be documented as legitimate and justifiable.
- Web experts routinely discuss Web 2.0 as a real entity (e.g., doctoral degreed persons, and Web implementers or operators). Web Forums endeavor to formally evolve Web 2.0 to make it more legitimate, to baseline its characteristics or enhance its capabilities (e.g., W3 Consortia).

- The father of the Web, Sir Tim Berners-Lee, stated that Web 2.0 did not exist; that what people call Web 2.0 today is a mere continuation of his original Web that he initially envisioned. He does not like the term "Web 2.0," those specific words or semantics, but he readily accepts the notion that "something," a Web continuation or enhancement, is indeed happening today on the Internet. Whether he chooses to call that "something" Web 2.0 or not does not really matter. Many other experts do indeed call "this Web continuation" by the name Web 2.0, if nothing else, only as a point of reference for their Web discussions. In the final analysis, it is just a game of semantics; which word or words to use to describe "what is happening today" on the Web, that "something" to which they all refer. Both "a Web continuation or enhancement" and "Web 2.0" are acceptable terminology to describe what is happening today on the Internet Web. Choose the one you like best, but "that something" does exist no matter what you call it, and it is rapidly evolving on a daily basis. The author chose to use the term "Web 2.0" since its use is more prevalent worldwide to describe today's Web environment, including its new social media and distinguished leading edge capabilities.

Based upon these facts, the various readings, and personal Web site observations, this research accepts the professional opinion that Web 2.0 does indeed exist. Now, the main frustrations associated with actually using "Web 2.0" are the facts that it is not yet formally defined, no consensus of opinion exists on its boundaries, and its general generation issue and the numbering of generations remains ill-defined. Adding to that confusion, Web 2.0 is not formally baselined or characterized by an authoritative body, so it can be definitively recognized "as such" when you see or encounter it, from all the other historical or technical segments, implementations or generations of the evolving Web. Web 2.0 is too complex for some people and a basis for heated argument. Given the belief and proof that Web 2.0 does indeed exist is not trivial to this research effort. Without it, the research would have no "heart" or basis to continue.

Knowing that Web 2.0 does exist allows for the formal analysis of collected data to be known as "Web 2.0 data" and the data analyses to be relevant to the research effort. It also provides a basis for the conclusions and recommendations as "legitimate statements" pertaining to "legitimate Web 2.0 items" (i.e., conclusions and recommendations derived from legitimate, real world Web 2.0 data). Thus said, Web 2.0 does exist and its data could be collected and analyzed, with legitimate output derived from those efforts.

Significant Web 2.0 data analyses are listed in the below paragraphs. Given the sheer volume of Web data and the enormity and scale of its data items, the author chose only those data relevant to the specific research goals and objectives, to directly answer the postulated questions.

B. DATA ANALYSIS CATEGORIES

1. Cost

No definitive cost summaries exist specifically for Web 2.0. It is not clear what Web 2.0 actually costs—single points of purchase or aggregate costs of products and services, infrastructures or architectures. Most budgets focus on discrete hardware, software and network components or personnel, and to some extent, general Web components (e.g., Web servers or Cloud Computing platforms). These are deemed Information Technology assets or relegated to the status of plain equipment acquisitions. Based upon Internet discussions and those costs observed in practice at military sites, initial Web 2.0 costs are anticipated to be moderate to high, $500,000 to $1 million or more. They should decline over approximately 10 years or so, provided it follows historical IT computer trends. Again, a pinpoint cost estimate cannot be affixed to an overall Web 2.0 environment; however, it is a Best Practice to strive to achieve that goal to effect proper financial management over time or to create future budgets. It is a good initial approach to sum what is known (e.g., technical components such as Web servers) and make allowances or rough estimates for the other parts of the Web 2.0 environment that are unknown (e.g., cost of services). Surveys of other organizations and their past experience with Web 2.0 appear to be helpful in cost estimating.

The Program Management Web 2.0 cost challenges: Identifying, submitting, and retaining a specific Web 2.0 budget in time of peace, during war, and difficult economic times. Showing Web 2.0 funds traceability and Return on Investment to specific mission accomplishment or improvements over time will be a major challenge, but required. Not having or knowing an official baseline of what exactly constitutes a specific Web 2.0 environment makes these tasks virtually impossible. However, assumptions must be made and a pseudo-baseline, technical and non-technical, established to provide a starting point for a local Web 2.0 implementation. Course correction can occur later when more Web 2.0 experience or information is discovered. Discrete individual products such as Defense Information Systems Agency's (DISA) Cloud Computing platform can be cost estimated through discussions with DISA. The difficult task is deciding what exact products and services are mature, secure, and available to procure, and then amalgamating them all into a comprehensive Web 2.0 budget that is justifiable based upon mission or business endeavors. Few really understand Web 2.0. It is imperative to seek Web 2.0 training so cost estimates can be more realistic, and derived budgets legitimate and defendable. This research clearly indicates that top-level management needs this training, too, so they might better understand and decide intelligently upon the submitted Web 2.0 budgets they must review and approve. Successful Web 2.0 implementation and maintenance requires continuous funding, and as its usage grows, Web 2.0 appears to be a significant enabler for Mission Essential status that must be funded. Otherwise, you will have mission or business degradation.

2. Schedule

No definitive schedules exist specifically for Web 2.0 and no records are being collected or maintained to that endeavor; hence, there is no reference base. It is not clear what "total" Web 2.0 implementations, configurations, maintenance or training times might entail, their duration or timing or expertise needed to evaluate them. Generally, Web 2.0 is lumped into the normal pot of operations: general acquisition, maintenance, or Information Technology related assets. It is anticipated that, as personnel become more familiar with the Web 2.0 technologies, they can achieve the synergy the technologies promise (i.e., schedule reduction). It is imperative to seek Web 2.0 training

so schedule estimates can be more realistic. Past experience and Lessons Learned should be reviewed for relevance to current endeavors. Realistic, "Just in Time" schedules are best. Unfortunately, there will be significant trial and error, and inefficiencies in estimating and achieving the related schedules. But a schedule baseline must be initially estimated and corrected over time to approach and set its milestones.

The Program Management Web 2.0 schedule challenges: identifying, segregating, recording, and maintaining records on schedules specifically associated with Web 2.0; its discrete scheduled milestones, dates forecasted in the future; and time durations on its various activities. It will require resources to perform this Web 2.0 overhead task. It must be effective and efficient to conserve those resources.

3. Performance

No definitive source exists that details the impact Web 2.0 has on organizational performance, or to describe the actual discrete performance of a Web 2.0 environment or its individual technical and non-technical components. The general Web is viewed as useful since it is widely in use, operational efficiencies are being achieved, and it is performing in a desirable manner. Initial impressions and limited usage of Web 2.0 in the workplace have demonstrated that it is a force multiplier, one that promotes rapid problem solving, global team collaboration, social media, and much synergy. It is anticipated that, as personnel become more familiar with the Web 2.0 technologies, performance should be enhanced, and associated costs and schedules reduced. Management must ensure Web 2.0 capabilities are harnessed and accessed "For Official Use Only" in an effective and efficient manner. Employees and Managers must be trained to use the Web in a responsible and secure manner. They must know how Web 2.0 might relate to their discrete tasks and how best to use it to achieve the best results.

The Program Management Web 2.0 performance challenges: identifying, segregating, collecting, recording, and assessing the discrete performance of Web 2.0 components and it, in aggregate, the ability to articulate what performance enhancements Web 2.0 actually impart to their overall Program today and over time. Web 2.0 performance metrics must be established and periodically modified, and their results

evaluated individually and in aggregate. Web 2.0 performance metrics will be a challenge to determine, track, and report. It also costs to perform this overhead function. The old "garbage in, garbage out" pitfall must be avoided. Unfortunately, it is very clear that not using Web 2.0 to enhance performance would be a poor choice, placing the United States military and businesses at a great disadvantage in the global environment. China has already demonstrated great capability with IT, hacking, Information Warfare, and its use and control of the Web on an international basis. To ensure Full Spectrum Dominance, the United States must employ Web 2.0 in an aggressive manner to mitigate global threats and enhance its global position. That employment must be effective, efficient, and secure.

4. Technologies

Web 2.0 presents an almost endless list of technical and non-technical technologies that exist or are currently being modified or created on a daily basis. Newly emerging technologies are so rapid and their insertion into Web 2.0 environments is equally fast. New and innovative uses constantly arise due to global sharing of information worldwide and the synergy that people acting in concert create or generate. Web 2.0 technologies and boundaries might be ill-defined or not fully recognized or documented, but it is generally accepted in popular use. Current Web 2.0 technologies are numerous and in heavy use for personal, governmental, business and military endeavors. The best examples for the Web 2.0 technologies are its many diverse uses that demonstrate its varied capabilities, applications, and innovations: Army Knowledge Online, Amazon, eBay, YouTube, Facebook, MySpace, Craigslist, Wikipedia, del.icio.us, Skype, Flickr, Blip.tv, LinkedIn, dodgeball, GovLoop, and AdSense, etc. All are social media based and depend on collaborative behavior and information sharing. Web 2.0 utilizes both technical (e.g., computers) and non-technical technologies (e.g., leading edge processes such as Cost Estimating paradigms or Six Sigma quality implementations). Technical data shows that over 1,000 Web 2.0 tools exist, many free (e.g., tools at Go2Web20.net at http://www.go2web20.net/).

The Program Management Web 2.0 technology challenges: identifying and keeping abreast of the newly emerging technologies; their fast pace of evolution or modification, changing domain focus areas, their varied operational intended or actual uses; and the accepted means to infuse them into the Program infrastructure in a timely, affordable, secure and approved manner to include their certification and accreditation. DISA is promoting their Cloud Computing platform on a fast track to successful Certification & Accreditation. Organizational employees and managers must be trained on Web 2.0 and its many technologies. In addition, these technologies should be monitored monthly as they rapidly change, are updated or replaced. They also possess flaws that create security challenges. Subject Matter Experts are likely to be needed to stay current on these Web 2.0 technologies and to effect recommendations on what, when, and where to employ the new ones. Participation in online technology forums is central to extracting the maximum benefit for PMs. Caution must be exercised that only tested, approved and secure Web 2.0 technologies be used.

5. Process

No definitive process or processes exist specifically for Web 2.0 and no records are being maintained to that endeavor. An attempt has been made to identify and diagram general Web components (technical connectivity) and their component behavior. It is both a Lesson Learned and a Best Practice to use process baselines and quality management programs for all processes to better manage their cost, schedule, performance, and security. Lean Six Sigma or regular "full" Six Sigma is very popular today as a quality program, along with International Standards Organization (ISO) standards. When implementing new Web 2.0 environments or a discrete component, process assumptions must be made as a starting point, and tentative processes identified, approved, secured and configuration managed over time. Once an organization has more Web 2.0 experience, these initial processes can be improved. It would also be prudent to understand where in the mission infrastructure Web 2.0 fits or interfaces and what processes it impacts. A Mission Decomposition Analysis is recommended to both understand how and where Web 2.0 supports the organization, but also to assess and correct its Defense in Depth and IA COP characteristics to best suit your business or

mission needs. The unfortunate fact is Web 2.0 might be so integrated / invisible that it can not be easily separated out to assess its discrete process characteristics. Web 2.0 may have to be included as a part of another, larger military or business process as a sub-process or invisible as a supporting item that is without an assigned process of its own. Likewise, Web 2.0 may cut across traditional boundaries and support many processes simultaneously, both vertically and horizontally in the mission or business structure. Process management will be a major challenge and, if aggressively pursued, could be very costly and time consuming. In some circumstances, it may not be worth the effort when assessed against a return on investment.

The Program Management Web 2.0 process challenges: identifying, segregating, documenting, recording, monitoring, assessing and improving the processes associated with Web 2.0. Tailoring a general management or a quality management program to the ever dynamic Web 2.0 environment will be a big challenge, but a necessary one. Additionally, processes are intertwined and pathologically connected in real world mission and business endeavors, making them impossible to segregate as individual Web 2.0 processes. Some may also have local, national, and international threads as well. It may be most advantageous to manage Web 2.0 processes at a macro level to save funds and time, and to effect timely decisions. Subject Matter Experts are likely needed to better understand complex organizational, intra- or inter- organizational, or international processes related to Web 2.0. Currently, there are few experts. It is a Best Practice to engage in process management at some level for all processes, to include Web 2.0.

6. People

No person or groups of personnel were designated specifically as Web 2.0 people in the course of this research. Currently, there are few Web 2.0 experts and the ones that do exist are expensive to hire. However, technical personnel involved in the operation and maintenance of the general Web are known (e.g., Web or System Administrators) and becoming knowledgeable on Web 2.0. Likewise, organizational personnel who use Web 2.0 technologies at work or home are gaining expertise. They can help educate organizational personnel on Web 2.0 and its many uses, and exactly where within the

business or military structure to infuse the Web 2.0 technologies. Unfortunately, no detailed skill set exists that baselines what training or aptitude personnel must possess to implement or use Web 2.0 technologies. It is advantageous that most current, actual uses of Web 2.0 today using select applications such as Facebook or GovLoop are typically intuitive. Users typically find it easy to use "up front" features, but the "hidden" technical components (software, Web servers or firewalls, etc.) will require greater expertise. The author's experimentation on over 14 Web 2.0-type Web sites found this to be generally true; they are typically easy to learn and use, fun, and useful (e.g., Wikipedia). Unfortunately, not all people embrace Web technologies easily. It is both a Lesson Learned and a Best Practice to educate, create awareness and deliver training on new technologies such as Web 2.0, to ensure proper and consistent usage within an organization's infrastructure, and to show traceability to work accomplishment and to promote proper security when used.

The Program Management Web 2.0 people challenges: identifying, funding and training the required Web 2.0 skill set. Recruitment and retention of trained Web 2.0 personnel will be difficult as they are limited and in high demand. Training the Trusted Insiders on Web 2.0, proper and secure internal use, and the monitoring of trained Trusted Insiders during work to ensure they do not accidentally or intentionally degrade the internal Web 2.0 infrastructure or the organizational security posture are major challenges. Older managers and employees may resist using these new Web 2.0 technologies and will need Command emphasis and encouragement. Top level managers must demonstrate "buy in" and commitment to Web 2.0 to make it universally accepted and used with an organization, otherwise its efficiencies will be lower. All employees must use Web 2.0 in a consistent, approved, and secure manner to gain its benefits. Likewise, Web 2.0 must be effectively and efficiently managed on an enterprise level to avoid waste and to promote security.

7. Quality

No definitive quality policy or standard exists specifically for Web 2.0. However, it is both a Lesson Learned and a Best Practice to have quality infused in all processes,

whether it's a process for products or services. Improvement is always a goal; enhancements in cost and schedule reduction, and performance. Lean Six Sigma or regular full Six Sigma is popular within general Web environments as a normal business practice for improving quality and has applicability to Web 2.0 as well. Likewise, the quality aspects of Web 2.0 are important to management for budgeting, performance and security reasons. From an operational perspective, whether Web 2.0 quality is low, moderate or high at any given time, is crucial to the success of any mission or business, including its Defense in Depth or IA COP framework. Poor quality might mean mission or business degradation or failure. In minor cases, poor quality might mean the loss of resource efficiencies, personnel synergy, or disinformation within an organization. In military environments, it might manifest in injuries, deaths, lost battles or wars. High quality is desirable in all endeavors.

The Program Management Web 2.0 quality challenges: defining and setting the overall mission or business quality standard will be a major challenge. Baselining the various internal and external processes for each mission or functional area, identifying quality processes or mechanisms, assessing the processes and their quality over time, evaluating quality performance metrics, and the selection and implementation of the requisite quality processes that meets the organization's goals, objectives, and budget will be monumental. Quality is an elusive characteristic that is difficult to understand and manage over time. An initial macro level is recommended. All organizational personnel must be trained on Web 2.0 and its requisite quality mechanisms, and how to keep them current or improve them. Quality is everyone's business. Subject Matter Experts will have to be employed to better understand this area as Web 2.0 processes and quality can be complex and difficult to understand, requiring experienced guidance. This administrative overhead will be expensive and must be balanced with mission and business goals, but with the understanding that without high quality, the mission and business will definitively be impaired. Quality is not an item you can live without, but it must be affordable, relevant to your organization and provide positive results.

8. Security

No definitive security standard exists for Web 2.0 and security was a major issue for past Web environments (e.g., intrusions or internal misuse). Security is still critical to today's Web 2.0 environments as it is always a tradeoff between full mission accomplishment and constraints that degrade the mission or frustrate productive employees. Web 2.0's nature of openness, collaboration and information sharing does not foster the traditional tight sense of security. Whether it be the internal users misusing or abusing the Web 2.0 technologies for personal pleasure, profit, or espionage, or outsiders deliberately using the technologies for ill gains or spying on an organization, misuse is immensely difficult to monitor, detect and control. It is both a Lesson Learned and a Best Practice to have security over all that you do, whether it's a technology, process, or personnel process. Proper security must be in place for Web 2.0 environments. Likewise, the access to, or accumulation of unclassified data or low sensitive information, must be evaluated to ensure those data "aggregates" do not inadvertently become classified or expose Web or organizational vulnerabilities to potential hostile threats. Web 2.0 is great tool, but unfortunately, it does not discriminate between users, good or bad people. Security must always be established and maintained to ensure Web 2.0 meets mission and business expectations for Full Dimensional Protection. Personnel must be trained on Web 2.0 and its required security.

Likewise, unanticipated issues must have contingencies for a proper and secure reaction to anomalies that might occur today or in the future. Backup plans are critical. Routinely backed up Web data is also important, Web 2.0 data too. Once the mission or business is dependent on Web 2.0, that new relationship must be protected and redundancies put in place to assure Information Operations and provide Full Spectrum Dominance. Once dependent on Web 2.0, the loss of that Web 2.0 at critical times could be catastrophic. Contingencies must be established, coordinated, annually updated, and periodically exercised. Plan for the unknowns and mitigate their influences.

Evolving homegrown terrorists and international threats must also be identified and managed. The National Security Agency or U.S. Homeland Security might have to be engaged. Expert assistance, governmental or contractual, will likely be needed. Costs for this assistance can be very expensive.

The Program Management Web 2.0 security challenges: identifying, choosing, implementing, and maintaining the requisite required Web 2.0 security framework, technical and non-technical, commensurate with mission or business goals and objectives will be a major challenge. Ensure only secure, tested and approved Web 2.0 products and services are acquired and integrated within Programs. Once integrated, an adequate Web 2.0 Information Assurance Common Operational Picture (IA COP) must be in place over the Defense in Depth employed for that Web 2.0 environment to alert management, technical and security personnel to adverse conditions as they arise, hacker, accidental or environmental degradations. Current Certification and Accreditation must not be jeopardized. The Trusted Insider "gone bad" will remain a significant challenge for management. Likewise, the accident prone employee, the less motivated and attentive employee, or those that engage in workplace violence must be anticipated and mitigated. All facets of security must be addressed ranging from traditional physical security to electronic security or people security (e.g., Privacy Rights). From a Web perspective, the commonly known threats and attacks must be identified and mitigated. The use of data encryption and Common Access Cards will likely remain a first line of defense for all Web 2.0 users, and users must be trained to protect sensitive data transiting over the Web or stored at their workstations. Likewise, technical personnel in sensitive Web 2.0 positions, where they might have negative organizational-wide or Enterprise-wide impact to the mission or critical segments of the Web 2.0 environment, must be carefully chosen, trained, certified and monitored during the performance of their tasks. Trusted Insiders "gone bad" can have a dramatic negative impact on mission or business success. Continuous tradeoffs among security, funds, and mission accomplishment will be a major challenge for management over time.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSIONS AND RECOMMENDATIONS

A. CONCLUSIONS

1. Research Goals and Objectives Were Achieved

a. Researcher gained a basic understanding of Web 2.0, its concept, controversial issues, technologies and diverse uses. Definitions were identified and assessed with the past history of Web 2.0 discovered.

b. Researcher identified Web 2.0 challenges, benefits and issues, especially those that relate to Program Management.

c. Researcher identified Web 2.0 Lessons Learned and Best Practices.

d. Researcher identified the future directions Web 2.0 might take.

2. General Web 2.0 Conclusions

a. Web 2.0 does exist. It has benefits and issues including that it is not formally defined or baselined, and is poorly characterized, but an informal definition does exist. Much controversy exists on Web 2.0, what it is and what constitutes its various technologies and capabilities. However, there is sufficient information to employ it in an operational Web setting, provided its use is approved and secure. There were Web generations before Web 2.0 (e.g., Web 1.0) and there will be additional Web generations after Web 2.0, such as Web 3.0 and Web 4.0, etc.

b. The general Web 2.0 Program Management challenges fall into eight broad categories: cost, schedule, performance, technology, process, people, security and quality. Many of these challenges are traditional in nature and some unique because of the Web 2.0 social media aspect, the people element.

c. It is a good management practice to employ Lessons Learned and Best Practices for any Web 2.0 operational endeavor. They must be collected wherever they might be found and shared among the Web 2.0 environments.

d. It is a good management practice to have a quality program for all internal and external operations with a part of it dedicated to Web 2.0. The use of Web 2.0 performance metrics to assess and improve its operational characteristics is in its initial stage.

e. It is a good management practice to identify and infuse newly emerging technologies that enhance operations, such as those within a Web infrastructure. New technologies such as Web 2.0 help to overcome old challenges, present new challenges, and provide an opportunity to achieve operational synergism on a global scale if used wisely, securely and with prior command approval.

f. The use of the Web, and in particular Web 2.0 social media and collaborations, enhance mission and business accomplishment and promote the principle of war called Mass. Synergy is achieved through online cooperation and information sharing to mass or aggregate required data, information or knowledge to support DoD decisions, problem resolution, and operational requirements.

g. One of the key defining characteristics about Web 2.0 is its collaborative aspect, its social media. Collaboration relies on independent individuals voluntarily coming together to share information, or to participate as a "just in time group or project team" to solve problems. This collaboration must be monitored to ensure it is effective, efficient, and secure.

h. Web 2.0 presents unique Program Management challenges that might require innovative solutions and Subjective Matter Experts to identify and resolve them.

i. It is a good management practice to monitor Web 2.0 progress, its generation of technologies, capabilities and uses, and the generations that will replace it. The infusion of these new Web technologies, capabilities and uses must be accomplished in an approved and secure manner.

j. It is a good management practice to use only Web 2.0 proven and tested "best product or service" solution sets, technical and non-technical. The law, Command policy, Certification and Accreditation, or security posture must not be

violated. It is a Best Practice to know what you have, where it is, and how it is performing: its cost, schedule and performance characteristics. The use of Web 2.0 performance metrics is in its early stage.

k. The Information Age is here to stay. Web 2.0 is the current Web environment that primarily supports today's Information Age activities over the Internet and the Web.

l. The biggest threat to successful Web 2.0 implementation and secure operation is the Insider Threat. Other critical threats exist (e.g., Web browser attacks, Web site redirects and identity theft, etc.).

3. Specific Web 2.0 Conclusions with Answers to the Seven (7) JAP Objective Questions

All JAP research objectives were achieved: To determine the current and future, technical and non-technical challenges that Web 2.0 might present Program Managers based upon answers to these JAP objective questions:

a. Q1: What is the Definition of Web 2.0?

There is no definitive or formal Web 2.0 definition, but Web 2.0 is both technical and non-technical in nature. Many informal definitions exist, mostly opinions.

Web 2.0 is a global technical and non-technical environment or architectural framework of many diverse and leading-edge technologies and capabilities acting alone and in concert over the Internet or Local Area Networks, as well as internal Intranets. Its main characteristics are its interactive social aspect, and the fact that its users are empowered to contribute to or modify its online content, technologies and capabilities. Web 2.0 is basically a "Read and Write" online Web environment, but rapidly expanding its abilities through incorporating innovative uses of social media and collaborations in new ways not previously known. Web 2.0 is a perceived continuation of the past Web, it can be described using different terms and is described by many as the next generation of the Web after Web 1.0. However, many argue that point, claiming that generations do not exist at all. The founder of the Web, Sir Tim Berners-Lee says that

Web 2.0 is "only a piece of jargon." Hence, he says it does not really exist as a "generation" but is only a continuation of the past Web, but he acknowledges "something" new on the Web is occurring. Based upon data collected, the author presented data and analysis that Web 2.0 does exist, but is ill defined, rapidly evolving, and not fully baselined or characterized to the point that it can be readily recognized and fully implemented as such. However, one can get close to Web 2.0 informal compliancy. Current technologies, applications and Web sites associated with Web 2.0 can be identified and reviewed for potential use in any Program, but there is no formal way to determine "Web 2.0 compliancy." Thus, below is the author's assimilated Web 2.0 definition from the data analyzed during the research period of approximately one year.

Wikipedia defined Web 2.0 best. Wikipedia is itself a Web 2.0 technology located at **http://en.wikipedia.org/wiki/Web_2.0**, dated 1 September 2009. It was a global collaboration of Web experts that provided the online definition. It was one agreed to by the global consensus of those involved in the Web, past, present and those planning its future. It is appropriate to use a Web 2.0 implementation (technology) to define Web 2.0, as it is probably closest to that topic, and it used real worldwide Web experts to formulate the stated definition. That "online definition" is monitored on a daily basis to ensure its current and future accuracy, and is heavily configuration managed. The fact that Wikipedia is now globally recognized and in use more than most encyclopedias, indicates the quality of its information is deemed "first class" by most people worldwide.

Wikipedia's Web 2.0 definition:

> **'Web 2.0'** is commonly associated with web development and web design that facilitates interactive information sharing, interoperability, user-centric design and collaboration on the World Wide Web. Examples of Web 2.0 include web-based communities, hosted services, web applications, social-networking sites, video-sharing sites, wikis, blogs, mashups, and folksonomies. A Web 2.0 site allows its users to interact with other users or to change Web site content, in contrast to non-interactive Web sites where users are limited to the passive viewing of information that is provided to them. The term is closely associated with Tim O'Reilly because of the O'Reilly Media Web 2.0 conference in 2004. Although the term suggests a new version of the World Wide Web, it does not

> refer to an update to any technical specifications, but rather to cumulative changes in the ways software developers and end-users use the Web (para 1–2).

b. Q2: What was before Web 2.0? Was there a Web 1.0? What were the characteristics of the predecessors to Web 2.0?

During the early history and stages of the Web, the various iterations of the Web as it evolved were not labeled by generation numbers. Once the term Web 2.0 became popular during the period 1999–2004, people started referencing the Web "before Web 2.0" as generations with some using specific numbers such as Web 0.0 or 1.0, and some did not use such numbers. Although many people still claim that "generations" do not exist, and that Web 2.0 or any version of the Web, are merely continuations and enhancements to the past Web, the majority of Internet users and experts worldwide deem Web 2.0 as valid and that it is identifiable through its capabilities and characteristics.

Before Web 2.0, there were:

(1) Web 0.0: An experimental, self contained internal-only lab Web. No more than 2–3 computers on a small "hard wired" network that transferred files using early Internet protocols from the Advanced Research Projects Agency (ARPA). Data later transited their network called ARPANet (circa 1969) using crude Hypertext Web language support. This experimental Web was developed by Sir Tim Berners-Lee at the CERN in Switzerland in the early 1990s and was deployed on a limited basis afterward. Many became excited by the technology, and the Web rapidly grew in infrastructure and uses. Web 0.0 was an infant Web that grew into today's Web.

(2) Web 1.0: A read-only Web from 1992–1994 with static Web page content that used Mosaic or Netscape browsers to access static HTML Webpages. These pages had minimal animation and imagery, and were all hosted on the early Internet, an ARPANet continuation into the university and public areas. Previously, most site content was accessed via data files using the File Transfer Protocol (FTP) in mostly a manual online manner, without much dynamic interactivity. Early Search Engines such as AltaVista evolved thereafter to facilitate user access to online data and

information posted on distant Web pages. Advanced search engines followed (e.g., Google from Stanford University). Once users became comfortable with the early Web, they expanded its uses and capabilities. They applied it internally to their organizations to create Intranets and to access internal information in a private or public mode using Web pages. They also integrated links to their internal databases for dynamic data access and update. During this period, static HTML evolved to be more dynamic and interactive, and became known as Dynamic HTML (DHTML). Text movement (page content), animation, music and imagery became more prevalent and interactive. In the early to mid-1990s, Web 1.0 started to mature, and in 1999 was then referred to as Web 2.0 by some people. Additionally, newly emerging technologies such as XML (eXtensible Markup Language) after 1997 were developed to further enhance known Web capabilities. From there on, the Web advanced at an incredible pace; so fast that describing it at any "point in time" would instantly be outdated as it progressed. The boundaries (if any ever existed) blurred between Web 1.0 and 2.0 (with much overlap).

c. Q3: Where do Web 2.0 implementations exist today?

Web 2.0 exists everywhere today. Almost all Web sites today are either Web 2.0 based, use Web 2.0 technologies, or access Web 2.0 capabilities from other Web 2.0-enabled sites. Many Web 2.0 Web sites are commonly known: Wikipedia, Facebook, MySpace, YouTube, Twitter. Web 2.0 (or the "something" that Sir Tim Berners-Lee calls a "mere initial Web continuation") is quite abundant on today's Internet. That "something" (Web 2.0) is out there.

d. Q4: What are the benefits of Web 2.0?

There are many direct benefits to using Web 2.0 (cost reduction, schedule reduction, and performance enhancements), and indirect benefits as well (synergism, global or local project team collaboration, information sharing, and innovative expert problem solving). Web 2.0 benefits can be both tangible and intangible. Given the innovation and pace that Web 2.0 presents, the benefits are only limited by imagination; how or where you use it, or for what task to use a new application. Web 2.0 presents many traditional benefits and future ones not yet discovered.

e. Q5: What are the issues surrounding Web 2.0?

Many issues are associated with Web 2.0, both good and bad (e.g., cost, schedule, performance, technology, process, performance, quality and security). Formally defining Web 2.0 and knowing its many diverse technologies, boundaries, baselines and capabilities over time is a difficult task. Web 2.0 can be viewed globally or locally architecturally, technically and non-technically (products and services), and is a complex, rapidly evolving and changing entity. Knowing its official boundaries, what exactly constitutes it and where it starts and ends within an organization, is a major issue along with its internal and external security. Yes, the traditional issues still exist (cost, schedule, performance, technology, process, people, quality and security), and the not so traditional issues exist with Web 2.0: Trusted Insider gone bad, fast-paced technologies, terrorists, nation states, complex technical topics, newly emerging technologies, undefined management and control, and the new and evolving Web 2.0 DiD and IA COP frameworks and IT tools, and the Information Age. All are important, intertwined and must be managed and controlled "in concert" on a continuous basis. The best approach to Web 2.0 issues is to "Think global and act local" when engaging, implementing, managing, and controlling Web 2.0 in the work place, and never forgetting its social aspect (people are its greatest strength and weakness). There are issues yet to be discovered as we get more experience with Web 2.0 and its future generations.

f. Q6: What are the Web 2.0 Lessons Learned and Best Practices?

(1) DoD may restrict access to social Web sites much like the Marine Corps did. A DoD policy decision will be made in the 2010 timeframe, one that will affect Web 2.0 use within DoD. This DoD decision must be monitored and implemented. In the interim, the Services should be careful on how and to what extent they deploy Web 2.0 technologies should they have to revisit, restrict or delete those initiatives after the formal DoD decision on Web 2.0 access.

(2) Web 2.0 will present security challenges to organizations that employ its technologies. The Web has shown that it is not secure and that unintended or accidental sharing of sensitive information can have harmful effects. The

same is true for Web 2.0. Defense in Depth must be employed over Web 2.0 environments and an IA COP instituted to protect, detect, react, and recover from accidents or intentional abuse of Web 2.0 technologies, processes and people, and the information over its Web and networks.

(3) Web 2.0 costs are not fully known, but like any newly emerging technology, initial costs may be high and technically knowledgeable Web 2.0 personnel scarce. It is a Best Practice to research, test, and compare new Web 2.0 products and services. Budgets must include future cost considerations as Web 2.0 is rapidly evolving.

(4) Web 2.0's main advantage is the collaborative synergy it brings to an organization and its individuals, both in work accomplishment and problem solving. Properly used, Web 2.0 can expedite schedules and deliver higher quality products and services. Improperly used, it can decrease productivity and consume needed network bandwidth. In a worst case, misused, Web 2.0 can be detrimental to mission or business (e.g., denial of service attacks or Trusted Insider gone bad). Web 2.0 employee training and policy guidance must be implemented, along with annual refreshers.

(5) The technology suite within Web 2.0 is not formally defined or controlled. Newly emerging technologies, modifications to old technologies, and new innovative uses of old, current or new technologies rapidly occur, some authorized and some in unauthorized manners. Web 2.0 technologies, processes, and people must be monitored and the impact of Web 2.0 changes assessed for good or bad, and negative items mitigated.

(6) Formal processes do not exist for Web 2.0. Web 2.0 processes need to be identified, baselined, and managed using a continuous quality management program. Processes should be affordable, effective and efficient.

(7) Organizational personnel associated with Web 2.0 (managers, technical support and users) must be trained to use Web 2.0 in a proper business manner.

(8) The use of the Web, and in particular Web 2.0 social media and collaborations, can promote the principle of war called Mass if used properly. A "mass of experts" can be engaged to analyze and solve problems. Synergy is achieved through online cooperation and information sharing to mass aggregate required data, information or knowledge to support DoD decisions and operational requirements, whether in peacetime or in war. Thus, Web 2.0 has the potential to support DoD Information Superiority.

(9) Organizations should only use tested and proven Web 2.0 products and services to ensure they are effective, and work in an efficient manner consistent with organizational goals and policies. Considerations must ensure Certification and Accreditation are not adversely affected.

(10) Organizations should allocate costs to their Web 2.0 environments (network, products and services), and ensure budgets support their Web 2.0 operations on an annual basis. Return on Investment records should be maintained to show where Web 2.0 funds were spent and what actual mission or business value they provided the organization. Bona fide needs must be met and legal funding requirements followed.

(11) Relevant Web 2.0 products and services must be identified and incorporated in a secure, effective, efficient, and affordable manner at the earliest opportunity into all organizations. Early synergism and potential productivity are needed today to enhance military and business operations.

(12) Subject Matter Experts may be needed to support Web 2.0 endeavors. They are scarce and expensive.

g. Q7: What is the future for Web 2.0?

The future of the Web or Web 2.0 in particular, is difficult to forecast. It is too new, people are just engaging it, and it is evolving at an uncontrolled, rapid pace that is hard to understand, baseline or to predict its many changes and uses, good or bad. When its core component involves people (social media, etc.), the unpredictability increases tremendously. People are both a strength and a weakness. The use of the Web,

WWW or Web 2.0 will continue as we know it since it is so popular today and has shown to be very valuable. But how long that popularity will last or what will replace it, is unknown. It is anticipated the general Web, whatever iteration, will be in use the next 5–10 years. Web 2.0 will exist for some time during that period and beyond. Web 3.0 applications are already in use on the Web with ability to read, write, and execute content interactively. The generations are all a blur since no clear boundaries exist among them. They seem to overlap and become "mere continuations" of each other.

The research identified these potential futures for Web 2.0 and its various Program Management challenges (e.g., cost, schedule, performance, technologies, processes, people, security and quality):

- Web 2.0 stays the same with no changes as Status Quo, however that is most unlikely given past experience with the Web and information technologies.
- A mere continuation or enhancement of the Web, WWW or current Web 2.0 capabilities might occur as minor or major updates to its technologies or uses as generations may or may not come to fruition. This will occur.
- Web 2.0 may blur or evolve into Web 3.0, a semantic Web with better search capabilities. This has occurred.
- Web 2.0 may alone, or with Web 3.0 integrated, blur or evolve into Web 4.0, an artificially intelligent Web. This has yet to occur.
- Something yet to identified or known comes to fruition that totally replaces the Web, WWW, Web 2.0 and all the supposed generations. Something innovative and unexpected may arise out of an experimental lab or from some genius individual. While that may indeed occur, it is most unlikely to occur near term for another 5-10 years, but who knows?

B. RECOMMENDATIONS

1. Do not use Web 2.0 unless the Command or management approves it first. Exercise caution in any endeavor to integrate Web 2.0 into your current Program or infrastructure before access restriction decisions are made by DoD. Ensure all

understand Web 2.0 within your organization, its cost, schedule, and performance tradeoffs. Ensure Web 2.0 does not violate your Certification and Accreditation. Have contingencies in place to handle any crisis.

2. Use only Web 2.0 proven and tested "best product or service" solution sets, technical and non-technical. Ensure you do not violate the law, Command policy, your Certification and Accreditation, or security posture. Know what you have, where it is, and how it is performing, its cost, schedule and performance characteristics. Use performance metrics as appropriate. Engage the DISA Information Assurance Support Environment Security Technical Implementation Guides (STIG) to better secure Web computers and servers (e.g., Gold Standard).

3. Assign a Web Subject Matter Expert (SME) to the project team, be it full or part time or as a dual-hatted person. Engage SME as approved and collaborate on Web 2.0, within DoD and outside. Maintain proper Information Security at all times with civilians and military personnel (i.e., clearance and Need to Know enforcement when discussing data or information).

4. Align your Web architecture, especially the Web 2.0 architecture, with the DoD Technical Architectural Framework and its Section 508 Disabilities Act, and DoD access policy guidance for Web 2.0 (when it is published).

5. Train all personnel on Web 2.0, its overview, proper and secure use. Provide annual refresher and updated training as required. Employ an Information Assurance Common Operational Picture for your Web environment and its Defense in Depth framework.

6. Establish a Web 2.0 Management Plan and project team to oversee its operation, now and into the future. Generate a Web 2.0 budget and its tentative project milestones. Ensure the plan addresses all the major challenges: cost, schedule, performance, technology, process, people, security and quality; and that it mitigate risk.

7. Implement Web 2.0 today within your program but plan to transition it to Web 3.0 and beyond within one to three years. Have a Web Roadmap. Get Command approval and policy guidance along the way. Use a good quality program such as Lean Six Sigma to manage all Web 2.0 processes.

8. Address testing, security, performance metrics, and quality upfront in every discrete implementation step of Web 2.0, do them early on and continuously. Perform vertical and horizontal analyses in and across Web 2.0 topic areas and domains to identify and mitigate issues (e.g., cost, schedule, and performance problems, etc.)

9. Use the DISA Forge.mil capability early on in your Web implementation for its software development support. Use the DISA Computing Cloud platform as appropriate within your Web architecture since it has a fast track to Certification and Accreditation. These platforms offer a bridge of sorts between Web 2.0 and Web 3.0. Evaluate their use as these are early offerings and may or may not offer significant enhancements to your current Web operations.

10. In general, managing Web 2.0 will be much like "managing Jello," an inherently difficult, if not impossible task. If you use Web 2.0, you must manage and secure it over time. Don't underestimate the complexity and cost of that task, or ignore it. It will affect you in some way, directly or indirectly.

11. Have and use a Web 2.0 enterprise management strategy, top down and bottom up. Use quality and performance metrics to monitor, review and manage areas within that strategy. Ensure your Web 2.0 is effective and efficient, and secure as part of that strategy.

12. Have full organizational commitment. Get user and management "buy in." Ensure all within the organization have education, awareness, and training on Web 2.0, its intended authorized uses and requisite security. Make sure your Web 2.0 is funded today and in the future.

13. Collect and use Lessons Learned and Best Practices. Avoid mistakes and be effective and efficient, and secure. Start your own Web 2.0 Lessons Learned and Best Practices, and share them within and outside your organization.

14. Synergism on a global basis provides an overwhelming force enabler for both good and bad. Manage Web 2.0 wisely and understand it can be both good and bad. Mitigate its negative aspects.

15. Know and control the Trusted Insider threat. Use Defense in Depth against all threats, especially the hostile or outsider threat.

16. Research, planning and budgets must be identified and programmed for Web 2.0 and whatever follows Web 2.0. Be it continuations of the Web, minor enhancements, or major updates such as Web 3.0 or Web 4.0, etc. Research, planning and budgets must accommodate the future Web generations. Think beyond Web 2.0 today.

17. Ensure you always have adequate, validated data backups should your Web implementation become degraded, denied or destroyed. Your mission or business should not have a major failure because of negative Web operations. Redundancies should be in place to ensure continuity of operations. Use and exercise an offsite Continuity of Operations Plan (COOP) site.

18. Seek training on the Information Age and know how best to use Web 2.0 to achieve DoD's Joint Vision 2010 and 2020 goals and objectives for Full Spectrum Dominance, Information Superiority and Full Dimensional Protection, etc.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

AIFIA. (2005). *Information Architecture definition*. Retrieved March 2009, from http://aifia.ora/pg/about_aifia.php

AKO/DKO (2008). AKO/DKO Advisor Issue 36. Retrieved December 2008, from https://www.us.army.mil/suite/login/login.fcc?TYPE=33554433&REALMOID=06-b476a858-73dc-10a1-9a8e-832f882fff3d&GUID=&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=SMwMjEqv5sB44%2bpUfE3qs4QL2G7Q0LjAUZ221N62Zll%2bTwHPFwKZd8Wg%3d%3d&TARGET=SMhttp%3a%2f%2fwww.us.army.mil%3a81%2fsuite%2fportal%2fauthenticate.do

Australia.to News. (2009). *Future of the Web Will Web 5.0 Take Control?* Retrieved 15 July 2008, from http://www.australia.to/index.php?option=com_content&view=article&id=4940:future-of-the-web-will-web-50-take-control-&catid=92:david-tow&Itemid=122

Australia.To News. (2009). *Australia's News from Australia's National Web site*. Retrieved on 18 August 2009, from http://www.australia.to/About.html

AMC Electronic Message (2009). DA Washington DC//G-3/5/7//, SUBJECT: Public *Announcement on the Army's Guidance on Accessing Social Networking sites* (SNS). Published 17 August 2009 by AMC.

Answers.com. (n.d.). *WikiAnswers.* Retrieved April 2009 from http://www.answers.com/topic/wikianswers

Baum, K. (2007). Defense Systems. *The Six Fatal Mistakes to Avoid When Implementing a Performance*. Retrieved February 2009, from http://www.defensesystems.com/Whitepapers/2009/02/Six-Fatal-Mistakes-What-to-Avoid-When-Implementing-a-Performance-Management-Initiative.aspx

Berners-Lee, T., Handler, J., & Lassila, O. (2008). Scientific American Magazine: *The Semantic Web*. Retrieved 26 March 2008, from http://www.scientificamerican.com/article.cfm?id=the-semantic-web&page=2

Beizer, D. (2009). Defense Systems: *DOD likely to adopt limited social networking. The tools may be used on military-controlled networks, Navy CIO Carey says.* Retrieved 26 August 2009, from http://defensesystems.com/articles/2009/08/20/navy-social-networking.aspx?s=ds_260809

Beizer, D. & Corrin, A. (2009). *5 reasons why the Pentagon should (and should not) embrace social media*. Retrieved 1 September 2009, from http://gcn.com/articles/2009/09/10/dod-and-web-2.aspx?s=gcndaily_110909

Blossom, J. (2009). Content Nation. Wiley Publishing, Inc, Indianapolis, Indiana, 2009, paragraph 1, p. 131.

Chairman of the Joint Chiefs of Staff Instruction (CJCSI). (2003). *CJCSI 3151.01A, Global Command and Control System Common Operational Picture Reporting Requirements.* Washington D.C.

DiNucci, D. (1999). Cole20 Web site July 1999 issue of Print magazine: "*Fragmented Future*" about Web 2.0 vs. Web 1.0. Retrieved July 2009, from http://www.cole20.com/who-coined-web-20-darcy-dinucci/

Computer Security Resource Center (CSRC). (2004). *Common Criteria for IT Security Evaluation*. Retrieved March, 2005 from http://csrc.nist.gov/cc/

Department of Defense. (2009). *DoD Architecture Framework Working Group Definition and Guideline (DODAF)*. (Volume I). Washington, D.C.

Department of Defense. (2004). *The Department of Defense Dictionary of Military and Associated Terms*. (Joint Chiefs of Staff Publication 1-02). Washington DC.

Department of Defense. (1997). *Joint Vision 2010*. (Joint Chiefs of Staff Publication 2010). Washington D.C.

Department of Defense. (2007). *DOD Directive 8500: Information Assurance (IA)*. (Joint Chiefs of Staff Publication 2020). Washington D.C.

Defense Technical Information Center (DTIC). (2009). Global Information Grid. Department of Defense (1998). *Information Operations (IO)*. (Joint Chiefs of Staff Publication 3–13). Washington, D.C.

Defense Technical Information Center (DTIC). (2009). *Global Information Grid*. Retrieved March 2009, from http://www.dtic.mil/dtic/

Federal Computer Week (FCW). (2009). DOD wrestles with Web 2.0. Retrieved August 2009, from http://fcw.com/articles/2009/08/10/week-dod-social-media-security.aspx?s=networking_120809 .

The FreeDictionary. (2009). *Definition of Internet*. Retrieved March, 2009, from http://www.thefreedictionary.com/Internet

The FreeDictionary. (2009). *Definition of Information Age*. Retrieved March, 2009, from http://www.thefreedictionary.com/information+age

Government Computer News (GCN) (2009). *Forge.mil Key Part of DISA's Net-Centric Strategy*. Retrieved April 2009 from http://gcn.com/articles/2009/04/22/forge-mil.aspx

Government Computer News (GCN). (2009). *An Enterprise Approach to Web 2.0*, Retrieved on 23 April 2009, from http://gcn.com/Whitepapers/2009/04/An-Enterprise-Approach-to-Web-20-in-Government.aspx.

IA Newsletter. (2009). *DoDTechipedia…A Way to Collaborate*. Volume 12, Number 2, The DISA IA Technical Analysis Center, p. 4.

IATFF. (2002). IA Framework Chapter 1 and Chapter 2. NSA IATFF Version 3.1. Retrieved February 2009, from http://www.iatf.net/framework_docs/version-1/file_serve.cfm?chapter=ch01.doc

Information Warfare Site. (n.d.) ASDC3I CIO FAQ. *The Information Warfare*. Retrieved February 2009, from http://www.iwar.org.uk/rma/resources/c4i/faq.html

ComputerWorld. (2009). *Firms Face Security Pressure from Web 2.0 Survey Says*. Retrieved July 2009, from http://www.infoworld.com/d/adventures-in-it/firms-face-security-pressure-web-20-survey-says-590

International Technology Education Association (ITEA). (n.d.). *ITEA Glossary*. Retrieved February 2009, from http://www.iteawww.org/TAA/Glossary.htm

Kambil, A. (2009). Emerald Web site Article: What is Your Web 5.0 Strategy? *Journal of Business Strategy*. Volume 29 Issue 6, pp. 56–58. Retrieved 18 August 2009, from http://www.emeraldinsight.com/Insight/viewContentItem.do;jsessionid=DD515EF680BE0C88CD968590F94AC941?contentType=Article&contentId=1751796

Kossen. W. (2008) *William's Internet Blog*. Retrieved 15 August 2009 from http://willemkossen.nl/b/?p=122

Kabay, M. (2009). *Network World: ScanSafe's Annual Global Threat Report*. Retrieved 2 April 2009, from http://www.networkworld.com/newsletters/sec/2009/033009sec2.html?nlhtsecstrat=ts_040209&nladname=040209securitystrategiesal

Laningham, C. (2009). developerWorks Interviews: Tim Berners-Lee, 22 August 2006, Retrieved July 2009, from http://www.ibm.com/developerworks/podcast/dwi/cm-int082206txt.html

Microsoft. (2009). Microsoft Gov 2.0 Whitepaper: *The Way to Gov 2.0, an Enterprise Approach to Web 2.0 in Government.* Retrieved April 2009, from www.microsoftgovready.com

Marsan, C. (2009). NetworkWorld: The 10 Dumbest Mistakes Network Managers Make. Retrieved July 2009, from http://www.networkworld.com/news/2009/070609-network-managers-mistakes.html?page=2

Mitre. (2009). *CVE: Common Vulnerabilities and Exposures.* Retrieved March 2009, From http://www.cve.mitre.org/

Technology. (n.d.). In Merriam-Webster Dictionary. Retrieved March, 2009, from http://www.merriam-webster.com/

Newman, A. C. & Thomas, J. G. (2009). *Enterprise 2.0 Implementation*, New York: McGraw-Hill Publishers.

National Security Agency (NSA). (2002). *IA Technology Framework (IATF).* Volume III. Washington D.C.

National Security Agency. (2002). IA Technical Framework. *NSA IATFF Version 3.1*. Retrieved March, 2009, from http://www.iatf.net/framework_docs/version-1/file_serve.cfm?chapter=ch01.doc

Reader's Digest. (2009, August) *How to Be Polite on Facebook* by Unknown Author, p. 96. WikiAnswers (2009). Retrieved August 2009, from http://wiki.answers.com/about/

Rosenfeld, L. & Morville, P. (2002). *Information Architecture for the World Wide Web: Designing Large-Scale Web Sites* (2nd ed.). California: O'Reilly MediaRoseIndia Webpage (2007). Web 3.0 Definition, 2007–2008, Retrieved 15 August 2009, from http://www.roseindia.net/Technology-revolution/web3.0/web-3-difinition.shtml

Simpson, H. (2009). Review of Sankar, Krishna & Bouchard, Susan A. *Enterprise Web 2.0 fundamentals.* Indianapolis, IN: Cisco Press, 2009. *Information Research*, 14(2), review no. R345. Retrieved, July 2009, from http://informationr.net/ir/reviews/revs345.html

Siegfried, D. (2009). *Wikinomics Editorial Review*. Amazon.com Site. Retrieved, July 2009, From http://www.amazon.com/Wikinomics-Mass-Collaboration-Changes-Everything/dp/product-description/1591841933

SysAdmin, Audit, Network, Security (SANS). (2008). The Top Ten Security Menaces for 2008 report. Retrieved 13 March 2009, from http://www.sans.org/2008menaces/

Shiels, M. (2009). BBC News Web site: *Security Experts Eye Worm Attack.* Retrieved 31 March 2009, from http://news.bbc.co.uk/2/hi/technology/7973131.stm

Tapscott, D. (2009). *How Mass Collaboration Changes Everything.* Wikinomics Retrieved August 2009, from http://www.wikinomics.com/blog/

The National Infrastructure Advisory Council. (2007). *The Insider Threat to Critical Infrastructures*. The National Infrastructure Advisory Council's Final Report Directed by Homeland Security Secretary Michael Chertoff 16 January 2007.

The Fort Huachuca Scout. (2009, July). *Fort Huachuca gets connected.* Volume 55 Number 28, 16 July 2009.

TARR Web server. (2006). *United States Patent and Trademark Office Web site data related to Web 2.0.* Retrieved 11 November 2008, from http://tarr.uspto.gov/servlet/tarr?regser=serial&entry=78322306

World Wide Web Consortium. (2009). *About The World Wide Web*. Retrieved March, 2009, from http://www.w3.org/WWW/

Wattanajantra, A. (2008). IT PRO: *What will next year hold in the ever-changing world of IT security?* Retrieved 16 May 2009, from http://www.itpro.co.uk/609391/top-10-security-predictions-for-2009

Wikipedia. (2009). *Web 2.0.* Retrieved April 2009 from http://en.wikipedia.org/wiki/Web_2.0

Zscaler. (2009). Zscaler Cloud security Web Forecast. Retrieved April 2009, from http://www.zscaler.com/forresterwebcast20090409.html

Zielinski, D. (2009). *What's New With Web 2.0?* Toastmasters International Magazine. Mission Viejo, CA, 92690.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Brad R. Naegle
   Naval Postgraduate School
   Monterey, California

4. Michael Boudreau
   Naval Postgraduate School
   Monterey, California

5. David Jones
   U.S. Army Information System Engineering Command
   Fort Huachuca, Arizona

6. Carol Lewis
   U.S. Army Information System Engineering Command
   Fort Huachuca, Arizona